DIGITAL SOVEREIGNTY:

AN ESSENTIAL REQUIREMENT FOR NATIONAL SECURITY AND DEFENCE

INTERVENTION OF MR. PIERRE BELLANGER

AT THE INTERNATIONAL ASIA/MIDDLE EAST SESSION (SIAMO)

OF THE INSTITUTE FOR HIGHER NATIONAL DEFENCE STUDIES (IHEDN)

TUESDAY, NOVEMBER 10, 2015

What is the task of a Defence department? In a few words, secure territorial integrity and protect the population from armed aggression; guarantee sovereignty and political independence if they are at risk; and finally, assist in combating threats to national security, i.e. the life of the nation.

In this context, the development of cyberspace, its machines and its networks has highlighted a new category of dangers which are now under serious consideration by the Ministry of Defence and other public authorities, resulting in just as many predictive and strategic considerations as actual concrete operational action.

This new risk has therefore been added to existing fields of intervention so that the appropriate responses can be deployed.

But this is not the subject of my speech.

In effect, each sector in society confronting the digital network is adapting to come up with a sector-based response which is often pertinent. But the effectiveness and permanence of these efforts are fragile because they do not have solid foundations: their point of reference is the network. But we are not sovereign on the network.

The Internet is a global change which requires a global response. If this idea, which lies at the heart of digital sovereignty, is not understood, any partial initiatives are destined to fail in the long-term, including in terms of national security and defence.

The Internet and its IT environment do not just give the world we know a new dimension. They replace it.

And by replacing it, they call into question the very foundations of society: public order, national security and defence.

In effect, what becomes of territory, law, independence and sovereignty when a growing part of the life of the nation is transferred onto the network?

This is the challenge of digital sovereignty.

The central idea is as follows: without digital sovereignty, the role of defence can no longer be executed.

Digital sovereignty is an essential requirement for national security and defence.

My speech will therefore consider:

- The dynamics of the network
- The effect of the network on society
- The myths and realities of the Internet
- Digital sovereignty and the consequences of its absence: for society and national security
- The American model
- The network and States
- Digital sovereignty: a political decision
- Three areas of action to establish digital sovereignty

The dynamics of the network:

The IT systems which make up the network double their efficiency every year. Between 1995 and 2015, at constant prices, their power was multiplied by a million.

The execution speed of software, meanwhile, has progressed 43 times more quickly.

Therefore, over the last twenty years the combined performance of programmes and machines has multiplied 43 thousand billion times and, for systems alone, will double over the next 12 months.

This exponential duo of software and systems is multiplied in turn by the network effect.

The network effect rules that the value of a machine is proportional to the number of machines to which it is connected.

This can be understood intuitively: the value of a telephone is proportional to the number of people with whom it allows you to communicate.

One machine connected to nine others is worth 10^2 or 100 since there are ten machines in total. An eleventh machine is connected. The value of each machine then increases to 11^2, i.e. a 121.21% increase in value with a single extra machine.

Hundreds of thousands of machines join the network every day.

The number of machines and appliances connected to the network increased from 200 million in 2000 to 15 billion in 2015 and there will be 40 billion in 2020.

This is therefore an exponential trio: software, systems and economics. It is enough to make your head-spin and is beyond our comprehension.

It is hard to know what these exponentials actually represent. Take this as an example: fold a piece of paper in two and then in four, fifty times in a row. How thick is the final folded piece of paper?

The answer is surprising: 114 million kilometres or three quarters of the distance of the Earth to the Sun.

The network effect can also be applied to people.

Three billion people are connected, 40% of the planet already, and five billion are anticipated in 2020. Never have so many individuals across the world had so many possibilities and choices; so much information and communication. Never has there been so much IT power available to each person through a network.

Our emancipation is equal to the square of all the emancipations to which it is connected.

Human beings are a constant future. The improvement of each connected individual therefore increases our own value and that of all the others.

Humanity can therefore make an unprecedented evolutional leap with the network. This will change all of us, personally and collectively.

The network is our opportunity.

The effect of the network on society:

Activities, projects and investments seek the best return, i.e. the quickest increase in value. This is what gives them the network effect.

The network effect reconfigures society: IT machines are connected on a network: they are clusters of servers. The networks of machines are connected on a network: the Internet. Documents are connected on a network: the Web. People are connected on a network: social networks. And now the objects and captors, and our bodies which carry them, are connected in turn.

The network of IT networks, the Internet, gets more productive, efficient and quick every day. It is becoming the great concentrator of value.

It therefore captures the value of society, all industries and all services, because it replaces them through better productivity, a better return and, above all, better service.

The myths and realities of the Internet:

We have needed time, collectively, to understand the Internet.

First of all, here is what it isn't:

The Internet is not a stateless libertarian and globalised utopia. Although on the surface it appears to follow the Flower Power tradition of the 1960s, deep down its origins date back to the 1950s and the Cold War. The Internet is an extension of the American nation.

The Internet is not only the playground of talented entrepreneurs and young technology companies. For decades it has responded to America's unprecedented intent which is simultaneously political, scientific and military.

The Internet is not given to us free of charge. Its matrix and its engine are the industry of intelligence. Its first function is to collect information. As users, we are like the turkeys which probably think that everyone is busy looking after their well-being until Christmas arrives.

The Internet is not a singular phenomenon, outside the law because of its very nature. On the contrary: you will never have signed so many contracts to use its services with just one click.

The Internet is not virtual. It is constitutive of reality. Reality is what hurts. The Internet hurts.

The Internet is not a new sector of the economy or society. It is actually becoming the entire economy. The Internet has not been added to the world we know; it is replacing it.

The Internet is not a future reserved for people who love technology. It is our present and our daily life. From registering for the school canteen to the very existence of millions of companies, small or large, the Internet is indispensable for everyone today.

The Internet is not a lost battle from which we will be happy with the crumbs. In fact, there won't even be any crumbs. Actually, nothing has been played yet definitively.

Finally, the Internet is not a threat but our opportunity. It will be our main problem only if we don't know how to make it our main solution.

Digital sovereignty and the consequences of its absence:

For society:

Our machines, the networks, the programmes and the services we use do not answer to our laws.

One tragic example can illustrate this.

Last June a terrorist attack in Isère ended in the decapitation of the marketing director of an industrial gas factory and the criminal who carried out the attack posted a photograph of the decapitated victim on the network.

Publication of a photo of this mutilated individual constitutes a serious attack on his human dignity as well as his private and family life, both of which are forbidden by the law.

In France this right to human dignity is a principle protected by the Constitution.

But our Constitution and our laws do not apply to overseas social networks. They answer to their general conditions of use and, as a last resort, the law of their country of origin.

These services can leave particularly shocking images online as long as they do not demonstrate explicit support or are not accompanied by a direct threat against the people or groups of people identified.

As this cruel photo did not fall into one of these categories, it was left online and distributed on a number of social networks.

The French Government has no direct coercive power to apply the law. It cannot act or give orders in an emergency.

As for judicial procedure, it would collide with a request from the lawyers of these services for the French High Court to be declared incompetent and for it to be replaced by other jurisdictions, in most cases the North District of California and the Court of San Mateo County.

At that point, Justice would hesitate between contradictory jurisprudence. Meanwhile, the harm would have been done and would have been amplified with the power of the network.

Our authorities were therefore reduced to requesting that these services please remove the photo. One of them did so only after 12 hours and the second three days later.

12 hours; 3 days: this is an eternity on the network.

It is enough time for an enemy to achieve his aim of firing up public opinion.

Terrorism is a form of war, a war which removes the distinction between reality and the network. It is a war of information. A war on our territory.

How can you win a war when you don’t have any weapons?

This photo was seen on our national territory by our citizens and we couldn’t do anything about it.

Let us note that the main American social network is keen to enter certain markets from which it is currently excluded and it therefore immediately destroys any videos which contravene the authorities it is courting and closes the accounts of those which publish them.

But here in Europe the only rule is public powerlessness.

The absence of law violates the law. The absence of law is contrary to public order. The absence of law on the network is contrary to preserving freedoms.

Without law, without public order, without authority (either *de jure* or *de facto*) on the network, what remains of the Republic?

Digital sovereignty is the opposite of this powerlessness.

Digital sovereignty means controlling our destiny on IT networks. It means extending the Republic into the information-based immateriality which is cyberspace.

Without sovereignty, there is no public order and therefore no law. Without law there is no freedom. And without freedom, what else is there?

At the same time, our entire economic and social edifice is collapsing.

We are under foreign supervision on the network.

The formidable opportunity of the network is set to be compromised and end in the exact opposite effect: poverty, enslavement and destruction.

From such promise, only peril will remain.

In effect, all the value which is being transferred to the network, and which is multiplying, is leaving us to go elsewhere.

All the data which is the basis of this new economy is being siphoned off.

A report by the *Boston Consulting Group* estimates that between now and 2020 the personal data of 500 million Europeans currently being plundered will represent a thousand billion euros.

Work, ideas, jobs and wealth are being swept up and the country's entire ecosystem and social balance are being put at risk.

There are social networks in California and social welfare protection plans in Picardy.

What globalisation did to the working classes, the Internet is starting to do to the middle classes.

According to *Oxford University*, half of all jobs will be automated, i.e. replaced by machines, within two decades. Half!

Of course, new posts and skills will appear but how can the transition be funded if the resources created by the network are somewhere else, often in the Cayman Iles?

According to John Chambers, Director of Cisco (one of the main IT companies specialising in servers and networks), a third of all companies could disappear over the next ten years because of digitisation. The remaining two-thirds will try to become digitalised versions of their old selves but nearly half will fail. In the end, only a third of the surviving companies will remain because, having been successful in their digital mutation, they will then be subordinated to the powers of the network.

What will be left in the wake of such upheaval? Probably a society torn in half with a hyper-class propelled forward by the network and the broken, precarious masses fighting machines for the remaining work.

What will remain is a society at the hands of the big Internet players which will control the network by concentrating its productivity and its fortune. They will have become the new masters, the new States.

This digital regime is in the process of succeeding without our consent, an invisible, non-violent coup d'Etat, making us believe that its domination is a condition of progress.

The only space for our freedoms will be what the general conditions of use allow us as they will have replaced the law.

Public order answers to our right to vote. This new private order will only answer to its own interests.

Citizens will live in an information-based world which will direct their purchases and their choices without them even knowing.

A recent study has shown that manipulation of the position of the leading results on a search engine can cause the choice of undecided voters in the American primaries to vary by 20% in a single consultation.

The collection of health and behaviour data will lead to communities being aggregated by risk and therefore tear up what remains of the collective approach to mutualisation, whether that is for insurance, bank loans or, of course, social security.

To each according to his data. To each, trapped by his data, to become an equation to be milked or ejected from the system.

The network is based on a new form of solidarity which fragments traditional mutual assistance and cooperation. That's fine if it better serves each individual and the general interest. But if this new kind of solidarity sits outside the law and only answers to private objectives instead of maintaining the social fabric through distribution, it dismembers it until it pits one individual against another.

This is the future.

The absence of digital sovereignty is bleeding our country dry like an animal.

For national security:

If independence, sovereignty and a population are to be defended, they have to actually exist.

What is left to defend?

Territorial defence is designed to push back an enemy. But we're not being invaded by an army; we are being invaded by a territory: the network itself.

And our citizens are migrating *en masse* onto this network: an entire nation of digital duplicates has been incorporated like a wave of plastic debris in the middle of the Pacific, a stateless crowd of digital illegal immigrants whose very existence, deprived of law, depends on overseas nations.

And this multitude of cyber-migrants is continuing to grow, joined by large numbers of companies subjected to unconscionable contracts and whose turnover is vulnerable, without appeal, to the discretion of far-off digital platforms with irrational conditions.

How can you defend a piece of sugar which has been plunged into a glass of water?

So, we have entered the age of the networks.

Historic nation states are confronting networks of digital services whose power makes States of them. The capitalisation of the top five global Internet companies is 1,600 billion dollars with assets of hundreds of billions of dollars. Furthermore, with turnover of 65 billion dollars, a company like Amazon has revenue which is greater than the GDP of half the world's countries.

In 2011 Apple's turnover, 73.7 billion dollars, overtook the balance of the American Government Treasury for the first time. Apple's turnover in 2014 was 183 billion dollars and its stock market capitalisation was 700 billion dollars, i.e. 100 billion more than the American military budget for the same year.

Moreover, historic nation states are confronting immaterial economic powers: the financial masses which are exchanged annually on electronic networks: two million billion dollars, or 25 times the Planet's annual wealth production.

Finally, historic nation states are facing criminal organisations which are organised via the network: from globalised mafias to radical terrorist networks. Their organisation into polymorphic, elusive and evolving networks is their main strength.

So, we are on the network in a new situation.

The atom led to the concept of an impossible war through the probable mutual destruction of enemies.

The network engenders the idea of an impossible peace.

The constant increase in the number of people connected and the exponential growth in the power to damage individuals makes peace statistically impossible. We are in a state of impossible peace.

Each grain of sand could cause the beach to explode.

How can national security be preserved when, henceforth, it will be perpetually damaged and threatened from within by internal or external, undetectable and unidentified players?

Here the network is central as it will be henceforth each time.

But the machines, their processors, the operating systems which drive these machines, the programmes, the services we use and, finally, the encryption which protects the secrecy of information: this entire digital ecosystem answers to sovereignty which is overseas.

Consequently:

There is no more secrecy. All our actions, thoughts and words are transparent for others to see and therefore can be used to weaken and damage us.

And there is no tough IT system designed to be watertight on a global level which can prevent the disappearance of secrecy. The choice now is between efficiency and secrecy. If closed off from the network, the system loses its multiplying effect; open to the network (not currently controlled and therefore possibly hostile) and the closed system becomes vulnerable to all kinds of intrusion – be that through human error or negligence or through software weakness, these *de facto* pseudo-closed systems always end up being permeated by the network.

<u>We are in a state of forced transparency</u>.

The exchange of information with allies is increasingly asymmetrical. Although we still have field work and a few large physical networks, our secrets are being uncovered and devalued.

We are becoming dependant on information collected by others without any independent means of verifying its veracity or its integrity.

Collecting data on our citizens using the machines and IT services on the network on our national territory is increasingly beyond us. Information mainly leaves for servers on the other side of the Atlantic and consequently search and detection functions too often reveal conditional access to overseas databases.

This is vassalisation through information.

Without control over encryption, little by little electronic conversations in our country become impenetrable to the services in charge of national security.

Two terrorists use a popular messaging application on mobile phones protected by strong cryptography which we don’t have the time or the means to decrypt. What are they saying to each other? We don’t know.

We are becoming opaque to ourselves.

Machines can be controlled from a distance, unbeknownst to us. All kinds of manipulations are possible, multiplying mistakes, false leads and erroneous incriminations. There is no more proof, no more information, no more certain facts.

We can no longer trust the network.

Machines, detectors and smart weapons can be limited so that, deliberately, people or information escape control. Already, some drones block air zones which have become forbidden in their geolocation processors; sometimes, places they have flown over no longer even appear in the photos to the surprise of their operators.

The news has just shown that, unbeknownst to States and for a number of years, Volkswagen was able to equip 11 million vehicles with rigged software which provided false pollution measurements.

What hidden software is currently housed in our machines and our networks?

In the future, individuals or mechanisms could thus escape any electronic tracking by the very machines which are supposed to watch them.

We can no longer trust our machines.

Pyramid-type chains of command are particularly vulnerable to doctoring by networks and machines which could answer to hidden instructions or those coming from behind secret doors. Are orders really orders? Has the information provided been modified? Are undetected intrusions undetected because they are undetectable?

We can no longer trust ourselves.

From a military point of view, the Europe of the future must be seen as a mesh of millions of networked pieces of micro-intelligence. Captors and processors will be resonating everywhere. It will be impossible to act without constantly talking in depth and in confidence with this network. If the network plays against military IT, there is a risk of paralysis without resources or visibility, lost in a hallucinatory state. What do you do when your own nervous system becomes the enemy?

Finally, speed is of the essence here. Access to all machines and all powers of calculation is crucial. The more data you have and the more capacity to analyse it, the quicker you can go and the more time can be slowed down.

A fly's eye can manage two hundred images a second, eight times faster than a human. When it rains, drops fall eight times slower relatively for a fly than for a human. The fly weaves in and out of the drops. The acquisition and speed of data processing slows down the world.

Only this ability to slow down the world through processing will be able to compensate for the flood of information during large-scale action and therefore provide the means for anticipation and decision.

Without controlling the network, the initiative will be opposing and the fog of war will only be on our side.

The people, meanwhile, must be seen, through mobile telephones, as a dynamic network of tens of millions of pocket super-computers. They are under the control of an overseas power and we can only communicate with our own citizens to alert them or mobilise them with its approval. However, we cannot stop messages of manipulation, propaganda or disinformation on 70 million terminals.

An entire society can be disorganised from a keyboard and a screen. Flight corridors, cash machines, electricity networks, traffic lights, access to the internet, telecommunications, news sites and apps are all targets.

Drones can sow panic and a thousand other disruptions that we cannot even imagine can be unleashed everywhere by badly identified players and even more easily because we no longer have a hold over our networks.

Finally, soldiers: every solder has a good part of his existence on the network and a considerable quantity of information has been collected about him.

This immaterial and intimate self is suddenly the hostage of another power. Such vulnerability exploited by expert destabilisation programmes used on a large scale can disorganise entire units.

The weapons are not complex IT systems. The fighter jet *Rafale* for example has a hundred or so combined computers and is equipped with an enormous number of highly technical captors exchanging data. This represents numerous risks of malicious connections to a network whose logic could have fallen into enemy hands.

In this context, conventional military confrontations will no longer be the first blow but the *coup de grace*.

For these reasons, the battle is lost before it has even begun - whatever the will and courage of those who are fighting it.

A defence department cannot fulfil its role without sovereignty on the network.

No network sovereignty means believing in the illusion of a physical country where only the decor remains in an empty and already conquered world. Work, value, information and power will be dematerialised in overseas systems and lands. And this country of software is not ours. In a hopeless guerrilla war, we are trying to protect one fiction with another: our distorted weapons against adversaries who already won long ago back home.

Finally, it is to be feared that a sleepwalking population, which the public authorities have let collectively and personally become hostages of the network, dreads any kind of conflict with such uncertain stakes and therefore chooses to side with the new masters immediately.

This is the reality of our situation.

The American model:

The internet cannot be understood without looking in depth at its American roots and, consequently, recalling the history of this great and beautiful nation.

The United States of America was created from a brutal civil and colonial war which had already been lost. The rebel colonists caught between unbelievable British power, the far-off kingdom of France and an immense Spanish empire to the south only had the hope of hopelessness.

Against all expectations, this ruined nation, rich only in future land, emerged victorious from the conflict. This left an existential anxiety which it would turn legitimately into global imperial intent.

Born of the bourgeoisie and not the nobility, which made it mercantile and entrepreneurial by nature, from the beginning the American nation combined to rebalance its finances, its political destiny and its economic strengths.

However, two ideas clashed: that of Thomas Jefferson, who supported the smallest State possible, and that of Alexander Hamilton, a determined supporter of public action. The phenomenal rise of the American economy in the 19th century thanks to British investment and then increased by the discovery of gold in California, would give supremacy to Jefferson.

The crisis of 1929 forced the return of Mr Hamilton. But the United States as we know it today was created with the Second World War.

The American war effort definitively released the country from stagnation. At the end of the conflict, the United States represented half the world's GDP. Its domination was total.

Starting with the war economy, the Pentagon worked closely with other national security agencies but also with government aeronautical and autonomic agencies, and participated in the coordination of several thousand researchers.

Politically, the theory behind this new structure came from the man who led its implementation, Vannevar Bush, President Roosevelt's scientific adviser. From such cooperation came technology like computers, reaction planes, civil nuclear technology, lasers and the start of biotechnology.

A new economic and political model was being affirmed.

This was the birth of the military-industrial complex. The army was the main partner and its leading client. Commercial and military approaches were combined. Investment was massive, cooperation exemplary and financial interest major.

Together with the Manhattan project to make the atomic bomb, it also led to the creation of a hidden state within the State, infrastructure which did not have to report to anyone based on secrecy and the extra-constitutional omnipotence of the executive and therefore the President, the ultimate and sole master of the absolute weapon.

This combination of industrial power and secrecy would be considerably developed thanks to the Soviet threat. Nuclear dissuasion would provide the structure for the deployment of a thousand overseas military bases and the organisation of the air force. Civil and military intelligence agencies would take on a dimension unknown until then.

In 1957 *Sputnik*, the first artificial satellite to orbit the Earth, was not American but Russian. This was a thunderbolt and a shockwave. America therefore decided to combine military power and scientific research in a new approach in order to guarantee its supremacy through wholesale innovation.

In 1958 a new agency was created, the Advanced Research Project Agency or ARPA, which became DARPA with an additional D for Defense. Its current budget is three billion dollars annually. A second governmental agency, the National Science Foundation, or NSF, moved the new approach up a gear with an annual budget of 7 billion dollars.

Directly or indirectly, we owe a number of major IT innovations from the second half of the 20th century and the start of the 21st to the DARPA/NSF duo, top of the list being the micro-processor and the internet.

During the 1980s the Japanese IT industry for integrated circuits started becoming too dominant, marginalising the American company Intel which was then the world's 10th leading company in the sector. The American Government decided that losing control of processors was out of the question, both in economic and strategic terms. This led to considerable support for Intel which would be the engine behind the advent of popular micro-IT.

But it was the Clinton-Gore administration, between 1993 and 2001, which founded the new digital American state. The Executive was convinced that the network, and therefore the knowledge and information industries, should be at the heart of the new American approach.

Technological activism at the highest levels of the State therefore undertook to revive the United States through scientific and IT innovation. The renaissance of the entire American empire began in cyberspace.

And this extraordinary vision would be combined with the military-digital complex which had already been operational for decades, considerably strengthening it.

The famous Silicon Valley is the visible part of a public approach in which the administration, the army and the intelligence services have invested several hundreds of billions of dollars.

The last constitutional barriers and locks exploded with the terrorist attacks of 11 September 2001. The nation came together and united the internet industry and intelligence in a patriotic coalition to give birth to an intelligence industry.

The federal budget devoted to intelligence would reach one hundred billion dollars annually, of which more than 10% was devoted to IT.

Research funds, benevolent investment funds which guarantee the other investors, generously supported companies which had any kind of strategic interest. The CIA fund, In-Q-Tel, has already lent its support to more than a hundred new technology companies.

One registered global social network, a weapon of mass digitalisation, was able to burn a billion dollars before even having a solid business plan.

DARPA evolved in parallel. Its initial mission to create an innovation ecosystem destined to give the army an incontestable technological advantage was now broadened to the use of this technology for the economic competitiveness of companies which were useful for intelligence.

The Pentagon spends about 60 billion euros annually on research and development, irrigating an ecosystem of thousands of IT companies of all sizes.

Biometric identification, robotics, drones, virtual reality, combat simulation, artificial intelligence, geolocation, satellite mapping, voice recognition, distributed IT, brain modelling, captors, big data, cyber security, fraud detection, encryption: all these sectors and many others receive combined funding and research from the army and corporations. There is no longer any difference between military and civilian technology on the network.

The intelligence industry fuses the civilian and military dimensions so as to make them inseparable. People, budgets, projects, funding: the barriers disappear. The intelligence industry is a combination of the two.

Take the iPhone. The internet, to which the terminal is connected, has its origins in DARPA; the cell phone technology comes from the American army; the micro-processor and the cache memory are from DARPA; the micro hard disk comes from the Energy Department and DARPA; the compression algorithms (software automates to reduce the size of files) comes from the Army Research Office; the touch screen comes from the Departments of Energy and Defense, NSF and the CIA; the NAVSTAR-GPS comes from the Defense and Marine Departments, and finally the Lithium-Ion battery comes from the Energy Department.

To finish, let’s add that iOS, the Apple phone’s operating system, is derived from OS X, the Mac operating system with which it shares its roots. OS X was originally the MACH operating system designed in 1985 by Carnegie-Mellon University and funded by DARPA.

With regard to Google, the development of the search engine from 1995 to 1998 was not only an NSF initiative funded by NASA and DARPA but also came from the Digital Library Initiative or DLI, a strategic programme from the Pentagon and the American intelligence services which would play a particularly active role.

It received support from the Massive Digital Data Systems (MDDS) Initiative stemming from the intelligence services and supervised in particular by the CIA.

Google is the model of a combined civilian and military enterprise.

Google intervenes in several American federal state structures which are concerned with national security technology such as the Task Forces of the National Research Council, the Institute for Defense Analysis and the Defense Science Board.

Google cofinances research programmes alongside DARPA, the Office of the Director of National Intelligence or ODNI (a coalition of 17 intelligence agencies and organisations) and NSA: 170 of these programmes have been identified by a German researcher and 75 of them allegedly implicate Google employees directly.

Google is not alone. Microsoft, Adobe, Facebook, Amazon, Intel and nVidia are directly involved in American national security projects.

Finally, Google is intimately connected to areas of American influence and diplomacy through the intermediary of an impressive group of government and private organisations and associations.

Its role goes so far as to provide IT and political assistance for the destabilisation of sitting regimes. This was the case during the Arab Spring.

The Obama administration has taken on and amplified this hybridization and has made the main companies on the network the equivalent of the state-backed merchants of the India Companies in the 18th century which were sent out by European nations to conquer the world and its wealth. These digital network companies are direct extensions of the power of the American State.

The terrorist threat, real as it is, also serves as a pretext to the introduction of a platform of economic intelligence on a global scale, gathering information on everyone connected, individual by individual, company by company, first and foremost to strengthen the American economy and power which are one and the same.

It is a state of affairs which today falls under the remit of a State.

To such an extent, indeed, that the Snowden affair which lifted the lid on this intelligence industry and caused a global scandal did not provoke any denials, excuses or profound and long-lasting changes in policy from the Americans.

Just a cosmetic effort to make people believe that there had been a falling out between the administration and the digital giants about encryption.

The American model is a cyber-State in progress, a State which is being recast by the network: imperial and global; civilian and military.

For this first cyber-State, like the colonial empires of the past, the world is divided into dominions, lands to be conquered and rival empires.

The network and States:

So it is understood: the organic alliance between America and the network gives this union a major advantage. But not supremacy. Absolute domination requires the weakness of other nations.

And this is not always the case. States and the network have achieved their alliance in several countries and in two forms:

Either open to the global network and using it to their advantage, such as South Korea, Israel and Estonia.

Or closed, filtering the network to create an economically and politically protected ecosystem to the detriment of open access for citizens. This is the case in Russia but above all in China whose resulting digital giants have global ambitions.

The rest of the world, the internet third-world, has not achieved an alliance between the network and the State. South East Asia, Australia, Canada, India, the Middle East, Africa, Latin America and Europe are getting left behind. Some exceptional companies are succeeding though despite the handicaps. But they are very vulnerable because they depend so much on American services.

Digital sovereignty: a political decision

A State is defined by territory delimited by borders and on which it exercises a common law determined by popular will.

This supreme will, this independent control of its destiny, is sovereignty.

Digital sovereignty consists of continuing the Republic and its rights into the dimension of digital networks.

For those who fear that this approach is detrimental to freedom, they should know, for example, that the last French law on intelligence is less intrusive than the known functionalities of free messaging services on the internet and mobile phones.

For those who fear that this step will slow down progress and innovation, they should know that our current status as a digital colony is not the best position to be in to be inventive and change the current state of affairs.

In effect, a nice European idea, and there are many, will grow with the constant risk of being ejected or challenged by the very platforms which host it. If, against all expectations, it manages to assert itself the best outcome will be to join the approach of the overseas players with incomparable resources. And that is true for both companies and our most promising talents.

For those who see this as a kind of fallback nationalism or anti-Americanism, they should know that liberty is universal and that to defend it here, as a civic nation, is to defend it everywhere. It is, indeed, about helping American civil liberties associations. And, finally, our American allies are our friends. But even my best friend does not make my decisions for me.

For those who immediately conclude that it is impossible act alone at a national level, don't forget that although the top four internet services companies turned over more than 300 billion dollars in 2013, i.e. the GDP of Denmark, the world's 55th economy, France's GDP is ten times higher.

For those who consider that it can only be done on a European scale: they are right but not straight away. However, national initiatives, including judicial ones such as the right to data, can increase considerably in scale when they are implemented across Europe. Europe is the second stage, not the first. We will find allies at that time to support and strengthen our approach. The first will probably be Germany. Finally, we must build European sovereignty together: Euro-Sovereignty.

Lastly, they should know that many countries are aware of their absence of sovereignty on the network. The Snowden affair played an explosive revelatory role in that.

We must have the courage to assert ourselves positively before the United States.

Take Ecuador and 15 other countries in Latin America: they assert their *tecnologica soberania* to establish their digital independence and, initially, free themselves from commercial software licences, most of them American, to use open source software whose users can legally control and modify the programme.

Switzerland too has become aware of the danger and is investing in new protected civilian and military communication architecture to secure its communications and its data nationally. The Federal Council has given the green light to a *réseau de données sécurisées* (Secure Data Network or RDS) which will join the *réseau de conduite suisse* developed by the Defence Department.

A country like France, with the world's 6th military budget, is incapable of guaranteeing its citizens that their correspondence and private life will be protected; it is incapable of guaranteeing its companies that their intellectual property will be protected. And we leave these people, abandoned, to the data predators? And this is the eroded and betrayed economy that we are sending in to fight globalisation?

No single economic or social force can resolve this problem. The State is the only thing which can rescue our society which is being damaged in these shifting IT sands.

After the networks of resistance, we now need resistance to the networks.

Individual companies can no longer try to adapt in the old disorganised, cobbled-together manner. The public authorities, meanwhile, must no longer reason, as tradition would have it, on the basis of sectors, grants and infrastructure. Finally, we must stop expecting everything from start-ups, small companies which are part of the Californian myth we have wanted to believe in too much.

That is all in the past. Now is the time for urgency.

The internet is a political project which requires a political response.

Only a network can rival a network.

And our country has still not revamped itself around and with the network.

And our country has no sovereignty on the network.

Digital sovereignty is a State decision. A major political decision which will decide our future.

Three areas of action to establish digital sovereignty:

The conditions for sovereignty are territory and law.

1: Establish a territory

Can you have a territory on the internet?

If a country chooses to partially close itself off or filter access to the network, the challenge is simplified. But the price is restricted choice.

In an open society, the issue is more complicated.

Physical territory is defined by its borders: you are either allowed through or you aren't.

Immaterial territory is defined by its encryption: you either have the pass code or you don't.

On the network, the border is the encryption.

On the network, sovereignty is the IT code.

Encryption protocols must be under public control and defined by the public authorities. It is a question of individual freedoms and national security.

Finally, all encrypted data will remain subject to our laws wherever it is found, like American bank notes whose sovereignty is extra-territorial.

So we have a border: encryption.

What is the territory, the land, its substance? Data.

Data is all the information generated by the network's users.

2: The status of data

The status of data is an essential issue in sovereignty.

That is why it must be understood that data hasn't really been personal for a long time.

We see personal data like a bag of marbles. I take a marble from the bag without affecting the others and then I put it back.

In reality, personal data is no longer like marbles. The bag of marbles has become a ball of wool: I pull on one piece of data and it brings all the others with it.

Why? Because data is interconnected and forms a network. With a mobile application, you hand over access to your diary, your address book, your conversations...This is not isolated data but data associated in a network: an appointment, for example, involves a number of pieces of information connected between themselves; and this data not only concerns you but also all the other people who are involved in it.

Similarly, by correlation and probability it is possible to deduce information from one person about others. Information about people suffering from a specific pathology provides information about all those who have the same problem.

In fact, data belongs to all those about whom it directly or indirectly informs.

If a piece of so-called personal data does not exclusively provide information about its source but also someone else, it is no longer just personal: it is still personal to the person at its origin but it also belongs to the other people concerned, integrally.

Data is no longer solitary; it is interlinked and in law forms joint ownership, essential common property. Sovereign common property.

This is our territory in cyberspace.

Consequently:

Any exchange, collection, processing or preservation of data on national territory must comply with the following conditions in particular to be approved:

- Use the authorised encryption protocols. These protocols guarantee both the protection of private life and public order;

- Physically or judicially locate the servers on national or European territory. We are leaving Sacramento for Nanterre or Montpellier;

- Ensure that fiscal domiciliation and the source of the data tally. Taxes are paid where the data is collected. This is a process initiated through an international agreement which is underway. This is the key to financing the social cost of the digital transition.

Now we need a law.

3: Make the law the code

What is a law in the material world? The ban on crossing the road when the pedestrian light is red is subject to an individual's discretion. In cyberspace it is not possible to cross when the light is red and this is why it bears the name governed space. It is no longer the pedestrian's decision; it is a line of IT code.

In cyberspace, the law is the code.

In the material world, all laws answer to a founding text which determines how the State functions and is structured. This text is the Constitution.

In cyberspace, this central structure on which everything depends is the operating system, i.e. the IT programme which pilots each machine.

In cyberspace, the Constitution is the operating system.

And it doesn't matter which operating system it is: the operating system is as old as the network.

In the past, an operating system would ensure that the office computer or mobile terminal worked properly.

Today, the same software core can be found in all computers and mobile terminals (of course) but it is also in cars, houses, all connected objects, the chips in bank or health insurance cards, robots, captors, signs and finally the software infrastructure of entire towns.

These operating systems form a network and constantly exchange information. They become our interface with the internet, our intermediary with other people and the world. They are the smart access to the network and they control it.

Like the laws which support the Constitution, all applications and services depend on this network of systems.

We need a sovereign operating system. This will be our Constitution in the immaterial world. It will guarantee the security of data, individual freedoms, law and the economy of companies. It will mutualise resources and engage the entire nation in renewal and growth.

China and Russia have already announced their sovereign operating systems. The United States has three main sovereign systems which you probably use.

Some people will consider that an operating system is an impossible task. Do they need reminding that Android, the operating system promoted by Google and which today equips more than 80% of smart phones, was launched by a team of half a dozen developers with an initial budget of only six figures and from an open source Linux core which was a European initiative?

This kind of sovereign operating system, or SOS, will never work by force but because it is the best, the most agile, the surest, the most efficient, the most open, the freest, the most cooperative and because it abounds in initiatives for which it is not the competitor but the guarantor.

We will find it in the Vitale health insurance card to protect our health data and in our cars which will no longer be held hostage by software from companies which launch their own competing vehicles. The same will be true of our payment systems which will give public authorities new visibility on the national economy and will maybe, for balance, lead to a reduction in taxes specifically for users of the SOS.

With encryption, the interdependence of data and a sovereign system, we find the fundamentals which guarantee our Republic in cyberspace.

It is the return of law and public order on the network.

And, most importantly: we need no longer set security against freedom.

In effect, how can individual privacy, the foundation of democracy, be protected when this very privacy can become a weapon against the community? How can you protect yourself against bombs made at the polling booth?

Because we control the encryption protocols, digital sovereignty means that identities and the information collected about these identities can be encoded differently.

One key for identities; a different key for information.

It will be possible to sweep up a lot of information without decoding the identities.

Such specific decoding will be reserved for the Justice department or for specific cases of national security.

As an additional guarantee, the system of decentralised block chain databases used for virtual currencies like Bitcoin could be applied to our data.

Therefore, because the encrypted data will be accompanied by metadata on the history of its use, it will be difficult to highjack it from its authorised uses without leaving any traces.

Of course, we will not escape all danger and worry. We will always be vulnerable. But every day our courage will rely on a new confidence. We will no longer be like children subject to the desires of the grownups. We will be adults ourselves, masters of our destiny on the network.

Defence and national security will therefore rest on solid foundations: an open network with security and guarantees, a network of sovereign and controlled connected intelligence. We will always have enemies but henceforth we will be able to truly defend ourselves.

Today, the gauntlet of digital sovereignty has been put down.

Thank you.