2012 4th International Conference on Cyber Conflict
C. Czosseck, R. Ottis, K. Ziolkowski (Eds.)
2012 © NATO CCD COE Publications, Tallinn

French Cyberdefence Policy

Patrice Tromparent
Delegation for Strategic Affairs
Ministry of Defense
Paris, France
patrice.tromparent@intradef.gouv.fr

Abstract: Since 2008, France has initiated a proactive cyberdefence policy in order to remain one of the first nations in the cyber realm and to ensure its security. This policy testifies to the need for a global approach to cyber, which could be useful for countries trying to develop relevant frameworks and synergies to address the new challenges of cyberspace.
This article aims to describe and analyse this French official policy. It is based on up-to-date documents, most of them only available in French, and some not even published yet.
Every aspect of French cyber policy is taken into account, in particular the very specific mechanism to ensure the security of critical infrastructures. Indeed, France, which is an old centralised state, has built up a national cyberdefence authority which regulates not only the public sector, but also the private sector. Some other changes are also interesting to analyse: the ongoing process of transformation of the Ministry of Defence, and the complex links between public and private sectors. France also acts on the international stage, in particular within NATO and the EU, to build up multiple levels of cooperation between nations and to ensure a better regulation of cyberspace. In so doing, France has to reassess its traditional balance between national sovereignty and interdependence.
As a result, like many countries, France has to develop new concepts in order to address the global cyberspace challenges ahead as far as forms of sovereignty, legal and ethic issues and military operations are concerned, potentially bringing new opportunities for international cooperation.

Keywords: *France, cyberdefence, cyberstrategy, cyberpolicy*

1. INTRODUCTION

The first duties of a state are the protection of its citizens, the resilience of its society and economic and social progress. Communication and information systems have become the nervous systems of our modern society and are now essential for economic and social life. The French White Paper on Defence and National Security of 2008 states publicly that the security and defence of cyberspace are a priority:

> "France must retain its areas of sovereignty, concentrated on the capability required for the maintenance of the strategic and political autonomy of the nation: nuclear deterrence; ballistic missiles; SSBNs and SSNs; and cyber-security are amongst the priorities." [1].

Since then, France has initiated a proactive cyberdefence policy in order both to remain one of the first nations of the cyber world and to ensure its own security. The main evolutions are the ongoing implementation of a defence and security continuum, as well as the gathering of all the actors in order to address the multiform threats in cyberspace.

France also acts on the international scene to build up multiple levels of cooperation between nations and to ensure a better regulation of cyberspace. Cyberspace defence also raises questions about the new forms of sovereignty, the legal and ethical framework and military operations.

2. THE WHITE PAPER ON DEFENCE AND NATIONAL SECURITY AND CYBERSTRATEGY

Like many other nations, France publishes a global assessment of the geostrategic situation on a regular basis in order to determine the directions of major defence policy-making[1]. The White Paper on Defence and National security of 2008 identified for the first time cyberspace as a vital challenge for security and sovereignty.

A. National Awakening

1) The Emergence of a National Cyberdefence Authority

The development of the information systems, which are the nervous system of our societies, has been identified by France as a major vulnerability. As the *White Paper on Defence and National Security* [1] stated, *"information systems, which are the nerve system of our economic and social life, as well as of the operations of the public authorities, of the major energy, transport or food producers, or again the organisation of our defence, have made our societies and their defence vulnerable to accidental breakdowns or intentional attacks on computer networks."* All sectors of the nation are likely to be attacked, implying a brutal, deep and even durable destabilisation of the society: banking and financial systems, air and rail transportation networks, communication and media networks, energy and water production and distribution networks, state decision-making autonomy and governmental and military capacity of action. The security of these sectors has already organised against diverse threats, in particular terrorism, and has already imposed constraints on their public and private operators, called operators of critical infrastructures (OIV[2]). The French Defence Code states in its article L1332-1 that

> "[…] public or private operators which exploit some installations or use installations or facilities whose unavailability would seriously compromise the warfare or economic capabilities, the security or survivability of the nation, have to cooperate at their own expense […] in order to protect these installations, structures or facilities against any threat, particularly terrorism. These installations, structures or facilities are designated by the administrative authority."

These operators currently number more than 200 and are divided into seven sectors: state

1 1972, 1994, 2008 and probably after the national elections in 2012.
2 *Opérateur d'Importance Vitale* in French.

service; transportation; energy; health; communications; industry and finances; food and water management; space.

In addition to the daily massive attacks, generally poorly publicised in the media, many foreign examples have made the headlines: the paralysis of Estonia in 2007 showed the extreme vulnerability of digitised societies, while the war in Georgia in 2008 testified to the potential use of cyberspace in military operations.

According to the 2008 White Paper, the hypothesis of a large-scale IT[3] attack against national infrastructures is likely to happen in the next ten years:

> "Over the next 15 years, the proliferation of attempted attacks by non-State actors, computer pirates, activists or criminal organisations is a certainty. Some of these could be on a massive scale. With regard to attacks emanating from States, several countries have already mapped out offensive cyber-warfare strategies and are effectively putting in place technical capabilities with the aid of hackers. Covert attempted attacks are highly probable in this context. Massive overt actions are also plausible over the next fifteen years." [1].

The classic distinctions between state and non-state attack, as well as between the public or private status of the target, are blurred in cyberspace.

Drawing conclusions from this truly comprehensive, and not only military, nature of defence of the cyberspace, France created the French Network and Information Security Agency (ANSSI[4]) in 2009.

2) France Cyberstrategy

France has a long experience of inter-ministerial structures. Indeed, according to the Constitution[5], the Prime Minister is responsible for national defence. Under his direct authority, a Secretary General for Defence and National Security (SGDSN[6]) organises and coordinates all the ministries' policies relevant to this field. The ANSSI, which belongs to the SGDSN, saw its attributions enlarged in 2011: it is now the national authority for the defence of information systems. Thus, it has authority not only over the administration and public actors, but also over public and private operators of vital importance.

The ANSSI quickly proposed a national strategy [2] to give an orientation and to set priorities. This strategy is based on four objectives.

First of all, France must count among the top nations in the cyber effort in order to retain its strategic independence as well as cooperating at the highest level with other nations.
Then, France must guarantee its freedom of decision-making by protecting the information related to its sovereignty. Indeed, autonomy of decision and action supposes, in any situation, the confidentiality and availability of critical systems for information and communication. The indispensable security products, in particular cryptographic ones, must be nationally designed

3 Information Technology.
4 *Agence Nationale pour la Sécurité des Systèmes d'Information* in French.
5 Fifth Republic Constitution, 1958, article 21.
6 *Secrétariat pour la Défense et la Sécurité Nationale* in French.

or even produced.

Furthermore, considering French critical dependency on information and communication systems, especially on the Internet, every public and private actor must collaborate to guarantee the security and resilience of critical systems, in particular the equipments' producers and the operators of critical infrastructures.

Finally, beyond the control of cyberspace physical supports, security in this domain must be enforced. This task requires an important effort in the fight against criminality involving every actor: administrations, companies and citizens.

3) ANSSI Responsibilities

The ANSSI has a central role in this strategy. Responsible for the defence of information systems, its mission is to watch, detect, alert and react to computer and network attacks, in particular on governmental networks but also on the critical operators. In the case of a major IT attack against an administration or an operator of vital importance, the ANSSI can enforce defence measures, including the isolation of networks.

The ANSSI leads an operational centre for cyber defence (COSSI[7]) which is permanently watching sensitive networks and informs the CERTA[8] – the French governmental CERT. The ANSSI also assumes an important role in the conception, procurement and certification of trusted security products and services which are essential for the protection of the most sensitive networks[9]. It has elaborated a *Security General Framework*,[10] encompassing all the administrations.

ANSSI's growing power allows it to intervene in the most sensitive cases of cyber-incidents. It typically brought its assistance and savoir-faire into play in two very symbolic cases testifying to the high level of threat. In March 2011, more than 150 computers of the French Ministry of Economy, Finance and Industry were infected by a Trojan targeting documents about the G20 French Presidency. In September 2011, the French nuclear company Areva discovered a massive infection, which had lasted for more than two years and had potentially caused strategic damage.

B. The Case of the Ministry of Defence

1) The Specific Vulnerabilities of the Military Systems

Besides their instrumental information and communication role for the Ministry of Defence, the systems also condition the operational superiority of the armed forces:

> "information, as pointed out previously, is the key to all strategic functions […] In terms of operational military needs, in addition to the acquisition of information referred to

7 *Centre d'opération pour la sécurité des systèmes d'information* in French.
8 *Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques* in French.
9 Article 9 of the decree n°2005-1516, December, 8th, 2005.
10 *Référenciel Général de Sécurité* in French: set of rules drawn up by ANSSI and stipulated in Ordinance No. 2005-1516 of 8 December 2005 'on electronic exchanges between users and the public administration and between public administrations' that certain functions contributing to the security of information must comply with. This includes, among others, electronic signatures, authentication, confidentiality and times-tamps. The rules set out in the RGS are mandatory and are adjusted to reflect the level of security defined by the administrative authority concerning the security of the online services for which it is responsible.

under the 'knowledge and anticipation' strategic function, the object is to establish secure, reliable, protected and high capacity communications, from the highest level of the State down to those in the field." [1].

While these systems have to work at any time and, in particular, during exceptional circumstances, they face a double challenge. Designed for better interoperability and compatibility, many systems are based on Internet technologies, often designed without any security components. Thus, they can be victim of the very numerous widespread attacks on the Internet, the so-called 'background noise' of cyber incidents. For example, in 2009, the involuntary import of the Conficker Virus into the Navy network led to the temporary unavailability of this network while the virus was eradicated. But the logistical system of the Rafale combat aircraft, which is supported by that network, was compromised.

Furthermore, these military systems contain high-value information and contribute to the operational efficiency of the armed forces: they are specifically targeted by precise and tailored attacks, carefully planned and executed. These hostile actions can affect the systems and networks components of weapon systems: embedded systems, as well as the infrastructures or weapon platforms (including SCADA[11]).

2) The New Organisation of the Ministry of Defence

The Ministry has long experience in information systems security. But the increase of attacks and actors required a more proactive organisation, considering cyberspace as a new domain for warfare.

In July 2011, the Joint Concept for Cyberdefence [3] defined the objectives and principles of cyberspace control by the armed forces. The main goal is obviously to ensure an active and in-depth defence of information systems operated by the French armed forces for their homeland and overseas operations. But the Joint Concept also contributes to the continuity of the essential activities of the state and brings its support to French or foreign partners in the case of a major cyber crisis.

In January 2012, this concept was followed by a doctrine [4] aiming at organising the Ministry and creating an operational chain of command for cyberdefence. Broadly speaking, the Joint Chief of Defence Staff (CEMA[12]) is responsible for the employment and command of the armed forces. In cyberdefence, he is also in charge of the whole defence of the information systems of the Ministry. To lead this defence, a unique and centralised joint and ministerial chain of command is organised. A General Officer, directly connected with the Chief of Operations of the joint staff, is appointed to conduct the Defensive Cyber Operations (LID[13]) of the Ministry and to perform the executive management and coordination of the whole cyberdefence domain: organisation, human resources, procurement, etc.

This centralised organisation favours an exhaustive knowledge of cyber events and better coordination. The Joint Operations Planning and Command & Control Center (CPCO[14]) takes into account cyberdefence in military operations. Among the units dedicated to cyber, the

11 SCADA (Supervisory Control And Data Acquisition)
12 *Chef d'Etat Major des Armées* in French.
13 *Lutte Informatique Défensive* in French.
14 *Centre de planification et de conduite des opérations* in French.

Analysis Centre for Defensive Cyber Operations (CALID[15]) is in charge of surveillance of, analysis of and quick response to cyber attacks. True MOD-CERT, it is in close connection with the COSSI of the ANSSI (both centres will be colocalised in 2013) and it is the correspondent of the other allied military CERT.

3. INTERNATIONAL RELATIONS

A. Cooperation between States

The interconnection of networks, in particular via the Internet, raises questions around borders and principles of sovereignty. All modern states, including emerging countries, are now dependent on networks and, broadly speaking, suffer the same vulnerabilities.

Cybercriminals use the World Wide Web in order to commit trans-border crimes. By contrast, states have to manoeuvre to sue these criminals in a real, segmented world, where some countries do not recognise the illegality of cyber acts. For example, the French infraction of 'contestation of crime against humanity' ('Gayssot Act' of July 13th, 1990) is not recognised in most of the world's countries (in particular in the USA, in accordance with the First Amendment). Thus, a hacker can use a 'botnet' in order to block access to a website from different countries. By contrast, police investigators have to respect long multinational judicial cooperation processes. Public administrations and companies, as well as citizens, suffer the same vulnerabilities and the same attacks.

Thus, France is convinced of the added value of international cooperation to assure the best possible knowledge of emergent threats and to share solutions. To this end, the ANSSI, via the CERTA, establishes relations with its counterparts. Since September 2000, the CERTA is a member of the Forum of Incident Response and Security Teams (FIRST)[16] which includes more than 200 members, and takes part in the activity of the Computer Security Incident Response Team (TF-CSIRT)[17] (which is the coordination cell of the European CERT (Trusted Introducer Level 2 since March, 2002).

As a matter of fact, the CERTA is in touch with every country worldwide, except for a few countries in Africa and the Middle East which still lack the adapted structures.

1) NATO

The cyberdefence challenge was tackled at the Prague Summit in 2002. However, it was only stamped as a new official mission of the Alliance at the Lisbon Summit [5] in 2010. First of all, the cyberdefence policy aims at strengthening the NATO information system, thanks to the improvement of security standards and procedures, as well as a more centralised management. It was recognised a

> "necessity for NATO and the nations to protect the critical information systems according to their responsibilities, to share the best practices, to build up a capacity in order to assist, if required, the Alliance members to counter cyber attacks."

15 *Centre d'analyse en lutte informatique défensive* in French.
16 http://www.first.org/
17 https://www.trusted-introducer.org/index.html

Another objective is to strengthen NATO capacity to coordinate mutual assistance in case of an important cyber attack, possibly with projected teams.

The sharing of the burden between NATO and the nations, which are responsible for the protection of their own information systems, was defined in order to strictly delimit the perimeter of the systems to be shared. France, indeed, considers that the responsibility to protect national networks primarily lies with each ally.

The determination of a cyber action plan and the implementation of the adapted structures have happened particularly fast, testifying to the importance of the issue. The NATO Computer Incident Response Capability (NCIRC) should reach its full operational capacity as soon as possible. This equivalent of a CERT at NATO is the counterpart of the CALID, after the signature of a Memorandum of Understanding (MoU) between France and NATO in September 2011.

2) The European Union

Very early on, the European Union showed interest in new technologies. The European Commission initially considered cyber from the angle of the protection of critical infrastructures, as stated in many documents: the so called "i2010" strategy ("an information strategy for growth and employment", 2005), "Strategy for a secure information society", 2006, European Programme for Critical Infrastructures Protection (PEPIC), 2004 to 2007, Programme for crisis prevention, preparation and management in matter of terrorism and other security-related risks (CIPS), up to 2013.

But it still faces many hurdles. In spite of the adoption of the Lisbon Treaty in 2007, which would have led to a certain harmonisation thanks to the dissolution of the three pillars, the actors in charge of cyber issues are still numerous: six Directorates-General from the European Commission (DG Infso, DG Justice, DG Home, DG Entr, DG HR, DG JRC), General Secretary of the Council, EU External Action Service, Parliament, European Data Supervisor, European Network and Information Security Agency (ENISA), European Defence Agency (AED), Europol and the "common enterprises" (Galileo and Artemis; there is no common enterprise for information systems security itself). Moreover, those issues are dealt with separately, depending on the nature of the issue (protection of citizens, of economic or technological development, of critical infrastructures; fight against cybercrime; cyberdefence).

However, since 2004 the European Union benefits from a dedicated instrument within the European Agency in charge of networks and information security, the ENISA (European Network and Information Security Agency).

A unit for watch, alert and quick response at the disposal of European institutions (CERT-EU) should be entirely operational in May 2012, while the European IT agency for the area of freedom, security and justice, created on November, 1st, 2011, should be operational on December, 1st, 2012.

France widely supports these initiatives, which should increase security for the Member States and citizens of the Union. However, Paris regrets the lack of unity which hampers global

efficiency, and the absence of a military dimension, particularly critical in the case of any EU-led military operations. France also wishes to establish a stronger link between the EU and NATO, which have 22 members in common. The EU would take advantage of the advance of NATO in cyber, and would bring its own experience in civil crisis management.

B. World Governance

The transnational features of cyberspace make it a common space, just like space or the high seas. For now, the only binding international legal instrument managing relations between states in cyberspace is the Council of Europe Convention on Cybercrime, ("Convention of Budapest") [6]. This Convention was adopted in Budapest on November, 23rd, 2001, by the member states of the Council of Europe and their partners (USA, Japan, Canada, South Africa); it came into force on July 1st 2001. It was completed in 2003 by an Additional Protocol about racism and xenophobia via information systems. Up to now, 32 states have ratified this Convention. It imposes on the signatory states the obligation to set up a national legal framework necessary for the prosecution of crimes in and through cyberspace, and to set up judicial mechanisms of cooperation.

Other initiatives are beginning to blossom. On September, 12th, 2011, China, Russia, Uzbekistan and Tajikistan (members of the Shanghai Cooperation and Security Organisation) sent a "Code of conduct for information security" [7] to the General Secretary of United Nations, within the framework of the 66th General Assembly of the UNO. This code, insisting on the superiority of the national law in cyberspace, tries to legitimise a takeover of Internet governance by states in order to enforce their security in their 'informative spaces'. This proposal refers directly to a governance model which is more focused on contents (information) rather than on networks, considering information as a potential threat, and stressing the possibility for a government to challenge the political system of another state via the Internet. The initial intent of the submitting states was not to have this paper adopted during the General Assembly but to receive advice and comments, particularly from the perspective of the UN Group of government experts on information security, which will take place in August 2012.

Moreover, Russia considers the cooperation between States Parties as a legal form of espionage, and is dissatisfied with the condition of a consensus of all the Convention members for the admission of a state which is not a member of the Council of Europe. As a result, Russia followed up by proposing a "Convention on International Information Security" [8] in December 2011 during the international conference on security at Ekaterinburg.

These two 'information war' approaches raise obvious semantic issues. They oppose France and its Western partners, which consider governance in terms of 'information systems security', to the Chinese and Russian approach of 'information security', which could lead to an unacceptable censorship in cyberspace. For example, the project of a Code of Conduct equates the fight against terrorism with the fight against extremism and separatist activities.

Countries supporting these new proposals argue that there is a legal gap on the topic. They have not commented on the possible articulation of these proposals using the existing legal instruments. However, one can easily see a clear alternative to the Council of Europe Convention on Cybercrime, as far as these countries consider either the obsolete character of a ten-year-old

text (Chinese position), or the specific dimension of cyberspace which requires new rules in support of existing international law (Russian position).

Other initiatives have been launched in other *fora*, such as the ITU[18] or the OSCE[19]. But an initiative at the OSCE from the USA, which led the Cyber Steering Committee, would probably be rejected by China (a non OSCE member) and not supported by Russia; and the ITU, driven by its General Secretary Hamadoun Touré, wants to be involved in Internet regulation [9]. Its current orientation is not favourable to a universalisation of the Convention of Budapest and aims to support the Russian approach of "cyberarms" control. In consequence, they probably have less chance of success than a direct dialogue at the UNO, in particular through its Forum on the Governance of the Internet, the next meeting of which will take place in Geneva in February 2012.

However, the adoption of a resolution on cyberspace governance is still exclusively discussed within the First Committee of the UNO (Disarmament and International Security); this completely matches with the Sino-Russian proposals, and does not allow a more universal consideration of the cybersecurity issue. The meeting of the group of government experts (GGE) in August, 2012, where countries favourable to the Convention of Budapest will be a majority, but where Russia and China will have a blocking minority, constitutes an opportunity to discuss the Sino-Russian proposal and to reach a compromise. In contrast, a failure in this negotiation could fuel a logic of 'blocks', with numerous problems attached.

France's position is to support the Convention of Budapest, which offers a relatively loose framework for states and could contribute to the emergence of a consensus on a definition of the threat (cybercrime) recognised by all, even by the initiator states of the Code of Conduct. This base could then be enlarged to take into account the legitimate question of the nature of the information circulating on the Internet, related to personal data, intellectual properties, abuse of freedom of expression, paedopornography, etc., or international security issues.

4. CONCEPTS TO BE EXPLORED AND THE FUTURE OF CYBERSPACE

The surge in the use of information and communication systems is beginning to be seriously taken into account by numerous countries. However, many questions remain unsettled and new problems are appearing.

A. Public-Private Relationship

The private sector dominates cyberspace as the owner or the operator of most of the information and communication systems, as the designer and manufacturer of equipments, as the main user (through economic activity), etc.

1) Operators of Critical Infrastructures (OIV)

France has historically benefited from the legal instruments required to impose the necessary measures for the protection of critical infrastructures. It now needs to adapt them to the new challenges of cyberspace. A legal framework is necessary, but not sufficient: concrete and

18 International Telecommunication Union.
19 Organization for Security and Cooperation in Europe.

serious measures must be taken to ensure an effective security of the systems.

2) Security of Private Companies
Despite a general reduction of public jobs, the ANSSI staff is growing steadily, from 250 persons in 2012 to a target of 350 persons in 2013, particularly in order to perform its mission with private companies (even though it cannot guarantee the security of all the companies). To achieve those goals, a new organisation has been in place since April 2nd 2012.
That is why, in addition to legal measures and controls, the ANSSI also carries out advice and training. For instance, it promotes the concept of 'IT hygiene', which basically consists of implementing routine efficient security good practice, in particular, antivirus, passwords, security updates and appropriate administration procedures. The more complex technical and expensive solutions are only applied to counter targeted attacks.

3) Support of Private Sector
The role of the private sector is crucial in the development of the Defence Technological and Industrial Base (BITD[20]). As France wishes to maintain its ranking as a world-class country in security technologies, it has to set up tools enabling the private and public sectors to collaborate and improve their good practice together. This approach is gaining traction, but the shape it will take is not yet determined.

Beyond timely collaborations in the support for research and development as well as shared educational programmes, a promising path may be the creation of a hub gathering all the actors, based on the model of the cyber security hub proposed by the British cyber strategy [10].

B. Doctrine Issues

For defence, cyberspace is a source of new threats but also of opportunities. All the operation concepts have to be reviewed to integrate this new dimension and all the planning processes have to take it into account.

The rules of strategy and armed conflict are discovering a new field of application. As the *French White Paper on Defence and National Security* stated: *"as cyberspace has become a new action field in which military operations already take place, France has to develop a fighting capacity in this space."* [1]. The notions of "'cyberwar", "act of war", "dissuasion" have to be revisited, while the International Humanitarian Law and its principles (distinction between combatants and non-combatants, caution, proportionality, ban of unnecessary suffering) have to limit the use of cyberspace.

Last year, the French Defence University (IHEDN[21]), in partnership with EADS, created the "Castex Chair of Cyberstrategy" which stimulates high-level thinking on these concepts. At the level of the Ministry of Defence, studies are led by various institutions (Directorate for Strategic Affairs, Direction for Legal Affairs, Joint Centre for Concepts, Doctrine and Experiment) to take into account these new aspects of military action.

France also contributes to this thinking in international organisms such as NATO, and pays a

20 *Base Industrielle et Technologique de Défense* in French.
21 *Institut des Hautes Études de la Défense Nationale* in French, under the Prime Minister's authority.

close attention to the studies in ACT[22] and in the CCD COE[23].

C. The Future of Internet Governance

The properties of cyberspace call into question the concept of national sovereignty. Maybe John Perry Barlow went too far when he proclaimed the independence of cyberspace in 1996 [11]. Nevertheless, the traditional pillars of sovereignty face hurdles in mastering the dissemination of information streams.

1) Internal Sovereignty

Every state tries to control cyberspace, whether to guarantee the safety of its citizens (through the fight against cybercrime) or to enforce law and order (for instance, through censorship) On the one hand, the scope of the control depends on the openness of the regime. On the other hand, all states are confronted with the same technical and practical problems.

France views cyberspace as a neutral domain by default; only its use may deliberately cause damages and, as such, can be prosecuted. In particular, liberties as defined in the European Convention on Human Rights [12] have to be respected: freedom of thought, religion, expression, protection of privacy.

2) World Governance

The triangular relationship between states, companies – which are heavily present in cyberspace – and citizens – who use it massively – raises the issue of world governance striking a new balance in order to respect the rights and interests of every actor [13]. A promising framework for dialogue is the Internet Governance Forum, which allows real progress in international cooperation.

The lack of world regulation mechanisms, or the perceived illegitimacy of regulation itself, could fuel extreme behaviour from citizens (“Anonymous” is a famous example of the mode of action of “hacktivist” groups) and even lead to a sort of ‘balkanisation’ of the Internet, which would be segmented in regional networks and governed by different rules.

Although France is represented within the GAC (Governmental Advisory Committee) of the ICANN (Internet Corporation for Assigned Names and Numbers), it believes that the regulation of the Internet must be discussed and determined within the framework of the UNO and based on the principles of respect for individual freedoms.

5. CONCLUSION

In cyberspace as in other domains, France, which is a permanent member of the UNO Security Council and the fifth world economic power, wants to maintain its ranking. It has implemented a voluntarist policy to protect its critical infrastructures, to develop its security technologies and to integrate this new domain into military operations.

There are still considerable efforts to be made and this requires a real collective awareness on the part of all the actors: public and private sector and citizens.

France must also develop international cooperation agreements to share information about

22 NATO Allied Command for Transformation, Norfolk (USA).

23 NATO Cooperative Cyber Defence Centre of Excellence, Tallin (Estonia).

threats and solutions, as well as to promote the values of freedom and neutrality of the Internet. It is under this condition that 'the age of uncertainty or anxiety' [14] can become the age of prosperity and security.

REFERENCES

[1] *French White Paper on Defence and National Security*, 2008.
[2] ANSSI, *Information Systems Defence and Security: France's strategy*, February 2011.
[3] CICDE, *Concept interarmées de cyberdéfense* (CIA-6.3), July 2011.
[4] CICDE, *Doctrine interarmées de cyberdéfense* (DIA-6.3), January 2012.
[5] NATO, *Lisbon Summit Declaration*, November 2010.
[6] Council of Europe, *Convention on Cybercrime*, November, 23rd 2001.
[7] Shanghai Cooperation Organization, *Code of conduct for information security*, Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General (A/66/359).
[8] Russian Federation, *Convention on International Information Security (Concept)*, Ekaterinburg, Russia: International Meeting of High-Ranking Officials Responsible for Security Matters, 21-22 September 2011.
[9] Hamadoun I Toure, "The International Response to Cyberwar," in *The Quest for Cyber Peace*, International Telecommunication Union and World Federation of Scientists, January 2011.
[10] *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*, November 2011.
[11] John Perry Barlow, *A Declaration of the Independence of Cyberspace*, Davos (Switzerland), February, 8th 1996.
[12] Council of Europe, *European Convention on Human Rights*, June 2010.
[13] Milton L. Mueller, *Networks and States: The Global Politics of Internet Governance (Information Revolution and Global Politics)*, September, 3rd, 2010.
[14] David J. Betz and Tim Stevens, *Cyberspace and the State: Towards a strategy for cyber-power*, 2011.