

THE PRESIDENT OF THE COUNCIL OF MINISTERS

Having regard to Law 3 August 2007, n. 124, entitled "System Information for the security of the Republic and the new discipline

secret ", as amended and supplemented by the Law of 7 August 2012, n.

133, and, in particular, Article. 1, paragraph 3-bis, which provides that the

President of the Council of Ministers, after consulting the Committee

Interministerial for the security of the Republic, adopt appropriate

directives to strengthen the activities' of information for the protection of critical hard and soft infrastructure, with particular regard to cyber security and safety protection national computer, and art. 38, paragraph 1-bis, which provides that

the Government attached to the report on information policy safety and the results obtained, which submits each year to the Parliament, a national security document concerning activities' relating to the protection of critical infrastructure

tangible and intangible, as well as' cyber protection and information security;

In view of art. 4, paragraph 3, letter. d-bis) of that Act Aug. 3

2007, n. 124, under which the Department of Information security coordinates the activities' of research information aimed at strengthening security and cyber security national informatics;

Having regard to Article 1 of the Law of 1 April 1981, n. 121;

Having regard to the Decree-Law of 27 July 2005, no. 144, converted, with

amendments by Law 31 July 2005, n. 155 on measures urgent to combat international terrorism,

Article 7-bis, provides that, without prejudice to the competence of

information services for the safety, the competent bodies of the Interior Ministry ensure the IT security services critical information infrastructure of national interest

and the Decree of the Minister 9 January 2008, by which the aforementioned infrastructure have been identified and it 'was

provides for the establishment of the National Center computer crime

for the protection of critical infrastructure;

Having regard to art. 14 of Legislative Decree 30 July 1999, n. 300, entitled "Reform of Government, in accordance with Article 11 of Law 15 March 1997 n. 59 ", which gives, among other things, the Ministry of the Interior powers to Civil defense and the decree of the Minister of September 28 2001 establishing the Inter-Ministerial Technical Commission Civil defense;

Having regard to the legislative decree 15 March 2010, n. 66, on "Code military order "and, in particular, art. 89 which identifies the powers of the Armed Forces and the provisions and directives consequent governing the tasks related to defense cybernetics;

Having regard to Legislative Decree 1 August 2003, n. 259 entitled "Code the electronic communications "and, in particular, the provisions that rely on the Ministry of Economic Development skills security and integrity 'of public networks communication and electronic communications services to the public;

Given the Decree-Law 22 June 2012, n. 83, converted with amendments by Law August 7, 2012, n. 134, which established the Agency for the digital Italy, which are handled by, inter alia, the functions attributed to the Higher Institute for Communications and information technology in the field of security networks as well as 'those of coordination, direction and regulation already' entrusted to DigitPA;

Having regard to Legislative Decree of 7 March 2005, n. 82, with the Code digital administration and, in particular, the provisions in cyber security;

Given the inter-ministerial decree of 14 January 2003, so 'as amended by Decree 5 September 2011, which established the Observatory for the security of networks and the protection of communications;

Having regard to Law 24 February 1992, n. 225, "Establishment of National Service of Civil Protection;

Having regard to Legislative Decree 11 April 2011, n. 61, implementing the Directive 2008/114 / EC on the identification and designation

of European Critical Infrastructure and the assessment of need 'to improve their protection;

In view of art. 5, paragraph 2, letter. h) of the Law of 23 August 1988, n. 400;

Having regard to legislative decree 30 July 1999 n. 303, embodying

"Order of the Presidency of the Council of Ministers in accordance with

Article 11 of Law 15 March 1997 n. 59 ";

The Order of the President of the Council of Ministers 1 October 2012 entitled "Order of the general structures of the Presidency of the Council of Ministers ";

The Order of the President of the Council of Ministers on May 5

2010 establishing the National Organization for crisis management;

Given the motion approved on 23 May 2012, by which the Parliament has committed the government to put in place all appropriate

initiative to come to the constitution at the Presidency of Council of Ministers of an inter-ministerial committee with task of developing a national strategy for the security of the cyberspace, to define the general guidelines and directives to be pursued within the framework of national and international policy

in this area and to identify Finally, regulatory intervention deemed necessary;

Considered that, in the characteristics of the threat right Cybernetics as a risk to national security, it is necessary establish a national strategic framework, with the specification of

roles that various institutional components must exercise for ensure the cyber security of the country and the preparation of mechanisms of action and procedures according to an approach coordinated interdisciplinary, on more 'levels, involving all public stakeholders, without prejudice to the duties provided for in

current regulations for each of them, as well as' private operators interested;

Considered altresì 'necessary to create conditions, through the

definition and clarification of tasks and activities' of different

institutional components and also with the identification of bodies

national reference for the cyber security able to interact with the corresponding authorities 'foreign, so that' Italy can fully participate in different cooperation fora International, both in bilateral and multilateral framework, both at EU and NATO;

Given the current legislative framework, marked by distribution of functions and tasks with relevance to safety cybernetics among many institutional entities competent in different stages of prevention of harmful events in space cybernetic; elaboration of guidelines and technical standards safety; the defense of the state from space attacks cybernetic; prevention and prosecution of computer crimes; preparedness and response to events cybernetic;

Considered that, on the basis of the aforementioned legislative data, the definition of a national policy framework on cybersecurity should proceed according to a path of gradual and progressive rationalization of roles, tools and procedures with the objective of increase the capacity 'of the country to ensure the security of the cyberspace, where necessary even with interventions regulatory;

It considered that, in the immediate, the conditions have to be created 'cause, under current legislation, can be developed action integrated that puts the pooling of different powers institutional outlined by the regulatory framework, and also make sure, in a logical partnership, the full contribution, in compliance with the provided by law, also of its powers private operators, interested in the management of systems and networks of strategic interest;

Abuses which have occurred for these purposes the need 'to impart addresses so that 'it is to emerge an institutional architecture based the clear identification of persons called to intervene and the tasks entrusted to them, while respecting the competencies already ' assigned by law to the different components and mechanisms of interaction between them;

It considered that this architecture should be developed in three distinct intervention levels, of which the first political address Strategic Coordination, which entrust the identification of functional objectives to ensure cyber security and national security, including the production of a National Plan for the safety of cyberspace, and that this level should also oversee the study and preparation of proposals for legislation to facilitate the achievement of these objectives; the second support, in permanent nature, with connection functions in relation to all Administrations and regulatory bodies, in the implementation of objectives and lines of action indicated by the schedule National and provide, at the same time, to plan the activities' operational-level inter-ministerial and activate the procedures alert in case of crisis; the third level of the management crisis, with the task to assist and coordinate the activities' response and recovery of the functionality 'of the systems, making use of all relevant components;

Held that, under the level of support to the implementation National planning, must be regulated in a peculiar way, in view of their specificity ', activities' of security information with the objective of enhancing the attivita 'of information research and analysis aimed at strengthen cyber and information security protection, making use of the instruments and procedures of Law n. 124/2007 and, in particular, with the directives of the President of the Board pursuant to art. 1, paragraph 3-bis;

It considered that the organizational-functional model so 'outlined should ensure full connection, in particular, with the functions the Ministry of Economic Development and the Agency for Italy digital as well as 'the activities' and defense structures of cybernetic space of the Ministry of Defence, with those of the Interior Ministry, dedicated to the prevention and combating of computer crime and civil defense, and with those of the civil protection;

Considering that the law gives the Interministerial Committee for the security of the Republic (CISR) in Article 5 of Law n. 124/2007 tasks advisory, proposal and decision on addresses and purposes' general politics information security, as well as' processing of the General and addresses the fundamental objectives to be pursued in

framework of the information security policy and that, in Specifically, pursuant to art. 1, paragraph 3-bis, of the law, introduced by Law no. 133/2012, the CISR and 'heard purpose the adoption by the President of the Council of Ministers Directives in the field of cyber security;

Abuses which have occurred the need of having to ensure, in the field of cyber security, a solid and reliable linking mechanism between the information security policy and other areas Action that are relevant to this particular matter, and duty for this concentrate in a single body interministerial the organ of political and strategic coordination in address the field of cyber security;

Considered in view of the tasks assigned by law to CISR and composition of the Committee, to identify that body Interministerial same CISR, was attributed, in accordance with art. 5, paragraph 2, letter. h) of the Law of 23 August 1988 n. 400, the tasks mentioned above;

Considered that the CISR, in the exercise of these functions, must It is adequately and consistently supported by an activity ' investigation, analysis and evaluation, and for such purposes the interministerial committee can avail collegial body coordination established at the DIS, in accordance with art. 4, paragraph 5, the Prime Minister's Decree 26 October 2012, n. 2 laying down the organization and operation of the Department of the security information;

Considered altresì 'that for effective performance of the tasks CISR is attributed to the need to ensure qualified contribution of the scientific character of information, assessment and the proposal and that, therefore, it appears appropriate to establish at DIS training school as a dedicated body, which also entrust functional tasks to the promotion and dissemination of a culture of cyber security;

No perceived need ', for the implementation of the lines of intervention contained in the space security National Plan cybernetic, in particular for what 'regarding the preparation and The inter-ministerial planning for crisis management, which in parallel with the activities' information acquisition and

analyzes entrusted to information agencies covered by the Act No. 124/2007, the activities' of the different administrations and institutions carried out according to the statutory provisions find a home siding facilitates and promotes the conduct in coordination of attributions of each component;

Considered for this purpose, to provide for the constitution in via of a permanent nucleus for cybersecurity, to be set up at the Office of the Military Adviser to the President of the Cabinet;

finally considered that a further and specific need for coordination is raised with regard to the operational management of crisis and the adoption of the measures necessary to restore functionality 'of systems, requiring a clear definition of roles and procedures so as to ensure a decision-making process unit and,

At the same time, the interaction of the national bodies responsible for emergency management counterparts with existing bodies internationally, and that, for these purposes', should be provided for an inter-ministerial body to be activated in case of crisis;

It decided to establish such a body in the Interministerial Nucleus situation and plan referred to in the Prime Ministerial Decree of 5 May 2010 providing for a configuration, which "Interministerial Table cybernetic crisis ", the optimal functional crisis management cybernetic nature, and to have that that authority, for the aspects technical computer emergency response, makes use of the national CERT established at the Ministry of Economic Development under Legislative Decree n. 259/2003;

Heard the Interministerial Committee on Safety of Republic;

It provides:

Art. 1

Object

1. This Decree defines, in a single context and integrated, the institutional architecture deputy to the protection of National relation to critical infrastructure security tangible and intangible, with particular regard to the protection of cyber security and national security, pointing to such out the tasks entrusted to each component and the mechanisms and procedures to be followed for the reduction of vulnerability ', risk prevention, the timely response to the aggression and the immediate restoration of the functionality 'of systems in case of crisis.

2. The subjects included in the institutional architecture referred to in paragraph 1 shall operate in accordance with the already 'competences conferred by law to each of them.

3. The organizational-functional model outlined in the present Decree pursues the full integration with the activities' of competence the Ministry of Economic Development and the Agency for Italy digital as well 'with those carried out by the Ministry structures Defense dedicated to the protection of their networks and systems nonche 'to the conduct of military operations in space cybernetic, from the Ministry of Interior facilities, dedicated the prevention and combating of cybercrime and defense civil, and those of civil protection.