

Information Age Vulnerabilities and Risks: The Emergence of a National Information Strategy

LTCol Paulo Nunes
CINAMIL
Academia Militar
Paço da Rainha, 29
1169-203 LISBOA, Portugal
pfnunes@net.sapo.pt

Prof. António Grilo
INESC/INOV
Rua Alves Redol, nº 9
1000-029 LISBOA, Portugal
Tel: +351-213100226
antonio.grilo@inov.pt

Prof. Henrique Santos
Departamento Sist. Inf.
Universidade do Minho
Campus de Azurem
4810-058 GUIMARÃES,
Portugal
hsantos@dsi.uminho.pt

1. Technical Revolution and Competitiveness

The technological revolution and the broad dissemination of the Internet use have build a worldwide virtual communications system that raise the perception that we live in a “global village”. The human interactions are no longer influenced by geographic barriers and are mainly determined by access times and information resources availability. In this context, the networked society environment in which we live in can be considered not only connexion-oriented but also information-oriented.

Knowing that the technologic evolution can be seen as a challenge and as opportunity of convergence to higher patterns of economic and social development, several countries are now looking for new ways and opportunities to support innovation and enhance the adoption of emerging Information and Communications Technologies (ICT).

Information is the source of knowledge and can influence in a decisive way the value chain of modern organizations, affecting power relations and shaping the strategic space where countries are able to compete.

Due to a direct consequence of structural delays and “information exclusion” phenomena we witness the appearance of a “digital gap” resulting in a growing difference between countries concerning their social development and information access conditions.

The growing vulnerabilities and threats in the information domain intersect all the activities spectrum of modern societies, affecting several aspects of their “interrelationships spaces” in the political sphere but also in the economic, military and social areas.

2. The Emergence of an Information Strategy

In the framework of a global economy, enterprises face a highly competitive environment where they have to assure an information superiority position in relation to their potential adversaries or direct competitors. If the enterprises conduct their activities of *Business Intelligence*¹, according with ethic and legal principles, we can say that their activity can be seen as a *Competitive Intelligence*² activity.

¹ The *Business Intelligence* activity can be defined as the process conducted with the aim of retrieving, analyzing and managing of the information that could be of interest to the commercial activity of an enterprise.

² We understand *Competitive Intelligence* as the ethic and systematic process of retrieving, analyzing and managing information that could affect planning activities, decision making and the operations of an organization (Taborda, 2002).

Although, due to a globalized world, what is considered legal by a Nation State can be considered a crime by another State, making the application of the most elementary law principles by each individual State even harder³.

Cyberspace also reveals some regulation problems since the States have a mitigated capability to exercise their sovereignty in this virtual space. If in this domain the enterprises violate the Law and use some unethical procedures, that will configure a conflictual use of information that can be identified as an Information Warfare⁴ situation. The actions conducted in the Information Warfare arena (Denning, 2000; NSSC, 2003) can assume the form of social activism (cyber activism or cyber vandalism), criminal actions (hacking, cyber crime, cyber terrorism) or war actions (cyber warfare or electronic warfare).

Considering the Information Society arena, in which information competition and conflict take place, our purpose is to settle the logic background to implement and put in to practice a National Information Strategy.

Within the logic of defending National interests we can expect that actors with bad intentions will look for ways to manipulate and control the information that circulate in the communications networks of different countries, affecting their national security. When the fulfilment of major national objectives⁵ is at stake, the nation state will have to develop an "Information Policy" (figure 1) that will guarantee not only the structural convergence to the technological parameters of the Information Society, but also the security and protection of its Information Infrastructures.

If the "golden rule" that points to the fact that to each kind of coercion corresponds a different kind of strategy (Couto, 1988, 227), the information use as a form of coercion will give birth to a new and important area of the global strategy, the Information Strategy. Hence, as one of the Global Strategy components and subordinated to its objectives, the Information Strategy can be defined as:

- The art⁶ and science⁷ of the information⁸ development and its use with the aim to fulfil the objectives defined by National Policy.

Concerning the action style, the Information Strategy can support both a direct and an indirect approach. While an indirect strategy it gives sense and logic to actions conducted in the real world (physical), building a context, adding value and contributing to maximize its effects (Francart, 2000). As a direct strategy it is itself action because it shapes the information environment (virtual space) in order to achieve a desired outcome.

Considering the nature of the means employed and the different sectors that the Information Strategy aims it is possible to conceive two specific focuses: one essentially

³ The legal aspects of privacy and personal data property are good examples of what is referred. In the US personal data is freely transferred between commercial firms but in Europe that data is seen within the focus of the individual and personal rights of any citizen to his privacy.

⁴ Information Warfare encompasses all kinds of actions that we can conduct to preserve our information systems and resources from the exploitation, corruption or destruction and to explore, corrupt and destroy the information systems and resources of an adversary, in order to achieve an information advantage (FM 100-6, 1996).

⁵ The major National objectives or the ultimate aims of a Nation State are the well-being and the National Security.

⁶ This term is associated with the intangible aspects of the information use. Within the scope of information domain, we can not forget the major role that perception management plays in the context of a conflict. This fact will fully explain the importance that Sun Tzu attributed to the empirical, intuitional and emotional aspects enclosed in the word "art".

⁷ This term is essentially linked with the tangible, scientific and methodological aspects of the information use.

⁸ The information assumes, in this domain, the double role of resource and weapon.

military-oriented and another mainly directed towards a civilian output. Within this context, Information Operations⁹ in the military and civilian realms are conducted.

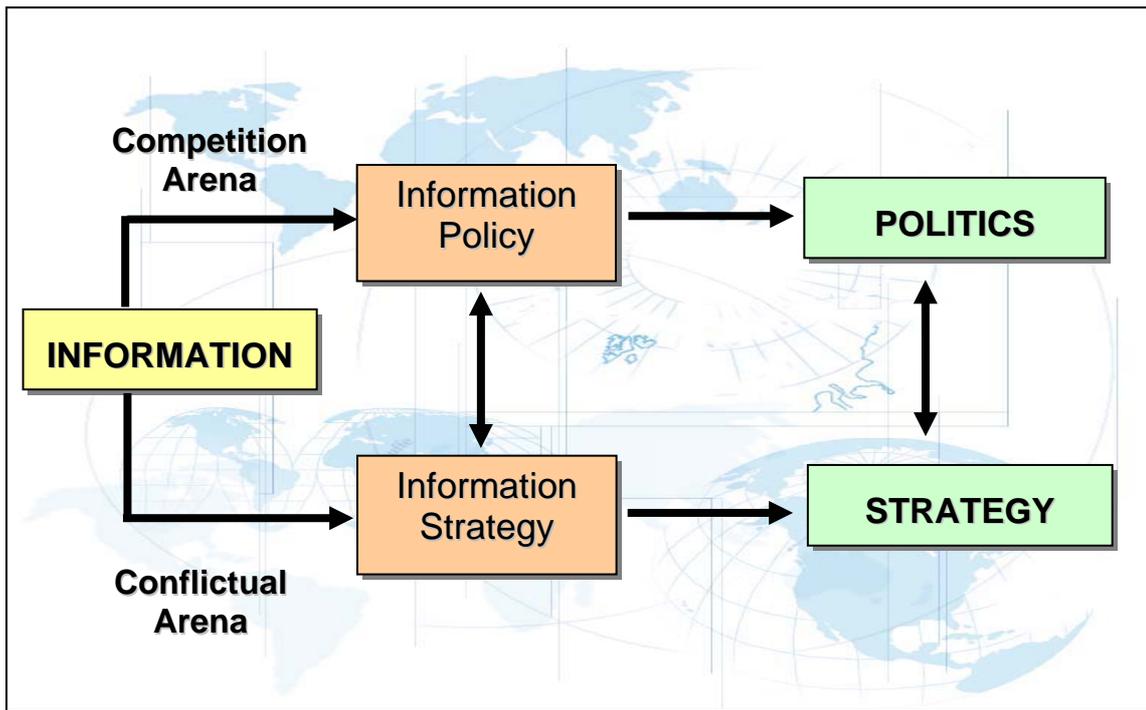


Figure 1- Conceptual framework of information use in competition and conflict arenas

In the Information Age the Information Strategy became a mandatory component in all domains of conflict influencing many of the traditional global strategy areas¹⁰: the weapon systems engagement (military strategy), the economic globalization and the digital transactions (economic strategy), the mass media and cyberspace activities effects in the perception management (psychological strategy), and the social networks and Internet-based public diplomacy (political strategy).

3. Information Warfare Weapons

Independently of its application context, the Information Warfare concept can be described as the use of information (resource) and the technologies that manipulate it (vectors) as tools (weapons) to assure the defence against adversaries. When trying to define this kind of warfare in the information domain, we may realize that some scenarios involving wars of hackers, electronic warfare attacks, cyber crime or even cyber terrorism attacks are being seriously considered by several countries and taken into account in their security and defence planning concerns. However, these approaches are normally the result of a vertical analysis that integrates in its rational only some specific and well-known capabilities not adjusted to the Information Warfare arena.

⁹ In accordance with the US Joint Publication 3-13 (1998), Information Operations are defined as “The aggregated activities and capabilities used to affect the information and information systems of an adversary and at the same time to defend our information and information systems.

¹⁰ According with LtGen Cabral Couto (1988), the main areas of the global strategy are: the economic, military, psychological and political strategies.

If instead of adopting a taxonomy based on the resources or the vectors that propagate the information, we differentiate these weapons in accordance with its effects, it will be possible to build an analysis matrix (Table 1) that will enhance a deeper understanding of its potential negative impacts. Thus, we may consider the existence of three major types of weapons that can be used to undertake an Information Warfare attack (Cohen, 1999), whose effects can be of physical, syntax, or semantic in nature.

| Weapons Effect | Attack Focus | Primary Effect | Type of Weapons (examples) | Model Complexity |
|-----------------------|---------------------|---|--|-------------------------|
| Physical | Physical | Denial of Service | Physical Destruction, Jamming | Low (linear) |
| Syntax | Structural | Blockade and logical operational corruption | Virus, agents, filters | Average (statistical) |
| Semantics | Behavioural | Affect the confidence of Systems users | Simulation of a false reality, Misleading Multimedia Information | High (chaotic) |

Source: Cohen (1999)

Table 1- Analysis Matrix of Information Warfare Weapons Effects

The use of weapons with physical effects presents low complexity and normally results in the permanent destruction of physical components of the information infrastructure, originating a system failure (denial of service). To accomplish this objective, we have at our disposal a wide range of means that include not only the traditional weapons systems of physical destruction, but also other non-traditional weapons as Weapons of Direct Energy. This last type of weapons is seen as a very important development because it allows the use of non-lethal force.

A syntax weapon aims to attack the operational logic of an information system, introducing unexpected delays or behaviours in its functioning. This type of weapons will also allow to acquire the control or to deactivate the logic of networks and information systems. Computer virus, normally used to produce this effect, constitute a good example of this type of weapons. Being the operative logic of the system its main target, the use of these weapons already involves a certain level of complexity. In contrast with the weapons of physical effects, there isn't the need to destroy the adversary's information resources or information systems. It will only be necessary to assure its control.

The primary effect to reach with semantic weapons will be the destruction or affectation of user's confidence in both resources and information vectors that carry it, modifying their behaviours. This type of weapons will seek to manipulate, modify and destroy the models that support the decision, influencing the perception and the representation of reality, constructed through the use of an information system. The complexity associated with this type of weapons is high, since it doesn't intend to affect the information system itself but the behaviour of its users, influencing its decisions.

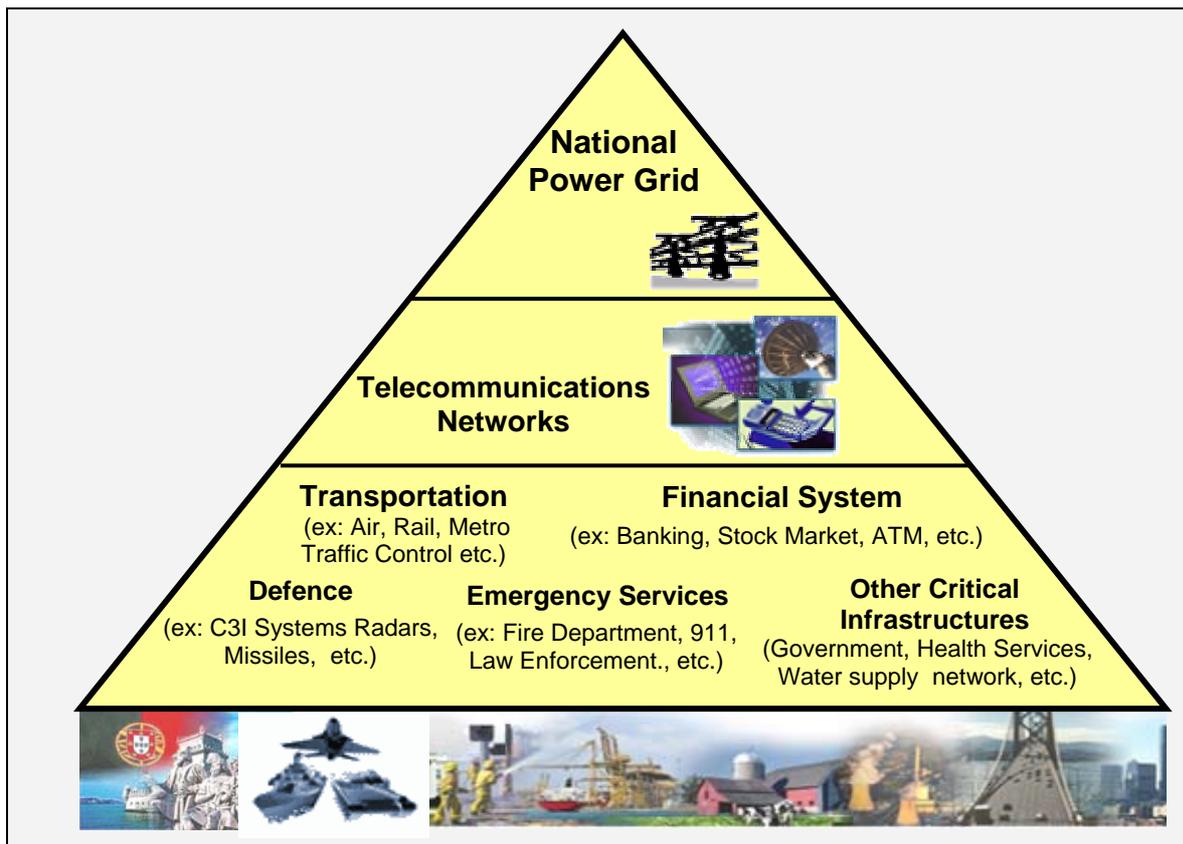
The growing dependence of organizations and States relatively to the use of open networks and automatic processing of data, as a form to retrieve, treat and share information, creates favourable conditions for the use of information weapons. At critical

moments of intensive information processing, as the ones that occur in a crisis or conflict situation, a selective attack to the information infrastructure of a Country may have unexpected consequences and a very negative effect on the safeguards of State's national interests.

4. The National Information Infrastructure

International communications networks blurred the traditional physical frontiers between networks and made it very hard to define the States' jurisdictional authority over them. Every country is confronted with the existence of a global information environment where it is not possible to clearly define what represents the National Information Infrastructure (NII).

If we think in the material resources that support this infrastructure¹¹, we may verify that it includes all the structures that support our daily activities. In fact, if we take as an example the National Emergency System (911), the Water Distribution System or even the Power Supply System we see the existence of an "interdependencies cascade" resulting from their interactions and the way their subsystems work (figure 2). If the information flows that are necessary for the correct functioning of all these systems are stopped, this situation will have catastrophic consequences.



Sources: Ramalho (2003) and Cardoso (2003)

Figure 2- Interdependencies Model of National Critical Infrastructures

¹¹ This infrastructure can be simply seen as an association of independent, integrated and interoperable systems (Herzfeld, 1999).

Organizations such as the European Union (COM, 2002) and some countries such as the US (NSHS, 2002; Lewis, 2002) and the Netherlands (Luijff, 2003), have undertaken serious efforts to analyse and identify the vulnerabilities of western societies relatively to the disruption of its critical infrastructures. Very often these efforts motivate a serious concern from the respective governments and stimulate the adoption of new policies. Even in Portugal, some signs of concern have recently appeared relatively to the fact that existent "critical infrastructures" could be attacked by terrorists. The government realized that if those infrastructures were attacked, that could compromise the well-being and the satisfaction of the basic needs of the population (DMDM, 2002; Caetano & Garcia, 2003). Following the general lines of existing studies on this theme (Ramalho, 2003; Anderson, 1999; Lewis, 2002; Cardoso, 2003), we arrive at a vertical model of functional dependencies, as the one presented in Figure 2.

Similarly to what recently happened in other countries¹², a long interruption of the electric power supply may cause a global failure of national critical infrastructures. The information infrastructure that includes the telecommunications networks will also depend of the power grid. Nevertheless, in other critical infrastructures case, there is a double dependency since these infrastructures will only operate if they are able to simultaneously receive their electric power (structural dependency) and the support of the information infrastructures they need to operate (functional dependency).

The NII's protection will require the identification of key-resources that have to be defended and preserved and an enhanced risk analysis and risk management processes intended to reduce the existent vulnerabilities (figure 3).

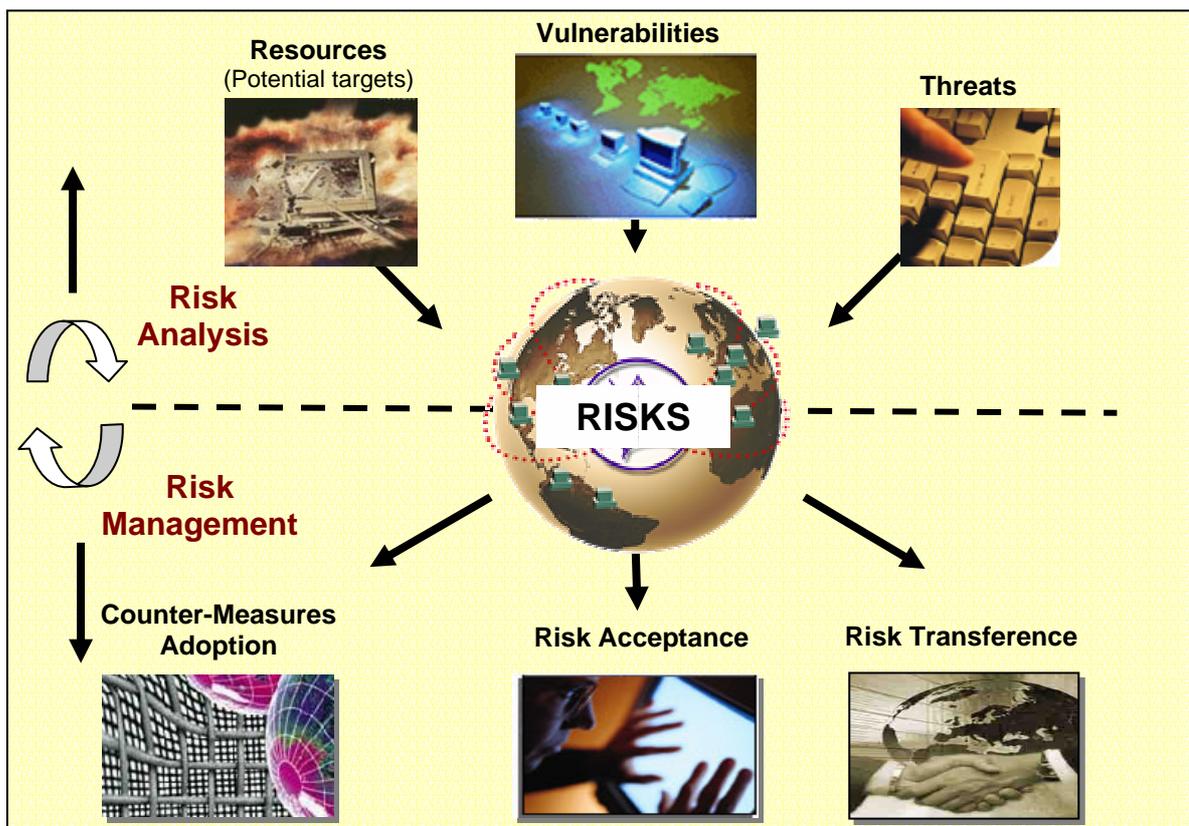


Figure 3 – Critical Infrastructures Risk Analysis and Risk Management Framework

¹² The electric power cuts recently occurred in the USA, Canada, United Kingdom and Italy, in the months of August and September of 2003, produced a strong impact in the critical infrastructures operation of these countries.

In the NII risk analysis process, we need to take into account the related effect of three major factors: the resources to be protected (potential targets), the information infrastructure vulnerabilities and the threats that may exploit the existent vulnerabilities and affect the resources we want to protect.

The risk management process can be put into practice through its reduction (counter-measures adoption), by doing nothing (risk acceptance) or transferring it to a third party. The choices associated to each of these three options will depend of the value assigned to the resources we intend to protect. The higher the criticality of a resource, the higher will be the need to adopt the necessary counter-measures to reduce the risk associated to it.

4.1. Information Infrastructure Vulnerabilities

Beyond the extremely positive aspects, associated with the use of the National Information Infrastructure, we can not avoid the fact that several services and information flows, vital to the regular functioning of governmental institutions, companies and the society as a whole, present today a very high dependence in relation to this infrastructure. In many cases, as already pointed out, critical infrastructures still present horizontal and/or vertical dependences, thus forming vital infrastructure chains. The disruption of such a chain of dependences will produce a "domino effect" of unintended and undesirable consequences. The failure of an infrastructure will be extended to the following ones originating the disruption of other infrastructures associated to it. Only the complete understanding of the true extension of infrastructure's interdependences (vertical and/or horizontal) will support the development of the appropriate and necessary countermeasures to correct and if possible control this effect. The fact is that these interdependences can be extended far beyond the sovereignty borders of the States, introducing an additional complexity factor to the problem.

The accelerated rhythm of ICT technical evolution also contributed to reduce the life cycle of these equipments. Due to a generalized public acceptance, most firms speed up its commercialization process, launching products to the market (hardware and software) without the completion of all the security and technical tests. This situation induces new structural and functional vulnerabilities in information systems and networks. Hence, information infrastructures will not only include different equipment generations but also equipments with potential bad functioning problems.

An attack conducted against the NII may have one or several of the following consequences: a loss of time to solve the current problems, a decrease of organizations productivity, large financial losses in consequence of firms losing market opportunities and reduced credibility, bankruptcy of commercial companies, the creation of instability conditions and social chaos, the paralysis of the transportation system, functional limitations of C3I Systems affecting the Armed Forces and Law Enforcement operational output, National Government discredit and, eventually, the loss of human lives.

The vulnerabilities currently presented by this Infrastructure and the existing mechanisms for its detention and correction constitutes a reason of major concern to "Information Age Societies". Within this context, efforts should be conducted to determine a Minimum Critical Information Infrastructure (National Emergency Intranet) that will allow focusing the protective measures on the safeguard of the vital information flows between governmental institutions and the diverse organizations/sectors considered critical for the survival of the State. Due to NII's central role in modern societies we can say that today "who controls the Critical Information Infrastructure of a State, dominates its Government and future outcome".

4.2. Threat Spectrum

The Information Era favoured the appearance of new "tools" that, when conveniently explored by hostile actors, allow them to develop a set of undesirable activities. Considering the basic principles that guide the risk management process, it will be important to also define the probability of occurrence of Information Warfare activities (Table 2).

| Information Warfare Activities | | Probability of Occurrence | Comments |
|---------------------------------------|---------------------------|----------------------------------|---|
| Offensive | Destructive (large scope) | Moderate | Restricted to few Countries |
| | Containment | Idem | Idem |
| Defensive | Destructive (large scope) | Reduced | Costs billions and requires a coalition of Countries. |
| | Containment | Moderate | Restricted to few Countries |
| | Preventive | Moderate | USA have already initiated this strategy in result of 11Set01 Attacks |
| Terrorists | Containment | High | Several terrorist groups. |
| | Preventive | Idem | Idem. |
| Criminals | Continuous | Very High | Subversive Activities. |
| | Random | High | Criminal Organizations. |
| | Random | Moderate | Small Groups or Individual Actors |

Source: Erbschloe (2001)

Table 2 - Information Warfare Activities Probability

Since threats can be seen as a result of the possibility of hostile actors exploring information infrastructures vulnerabilities, we will have to evaluate both the intentions and the capabilities of those actors to inflict damages to the NII (see Figure 4). The threat level can be derived from actions/attacks lead by isolated individuals (amateurs, hackers and crackers), by organized groups (organized crime, groups of pressure/lobbies and terrorists) or even by States.

The amateur's threat results from the conduction of sporadic actions that are not technically elaborated but aim to explore the increasing vulnerability of information infrastructures. Hackers normally possess greater technical knowledge than amateurs. These individuals also present a deeper knowledge of systems complexity and reflect the intention to violate the security mechanisms of networks and information systems. Hackers may present a great diversity of motivations, varying between those that are simply curious to break the systems defences to those that commit acts of vandalism. This last group is known as crackers.

The increasing interconnectivity of networks and information systems make them an interesting target for political dissidents and groups of pressure (lobbies). As an example, it is mentioned that the Internet constitutes today an important vector for the dissemination of political messages and social activism.

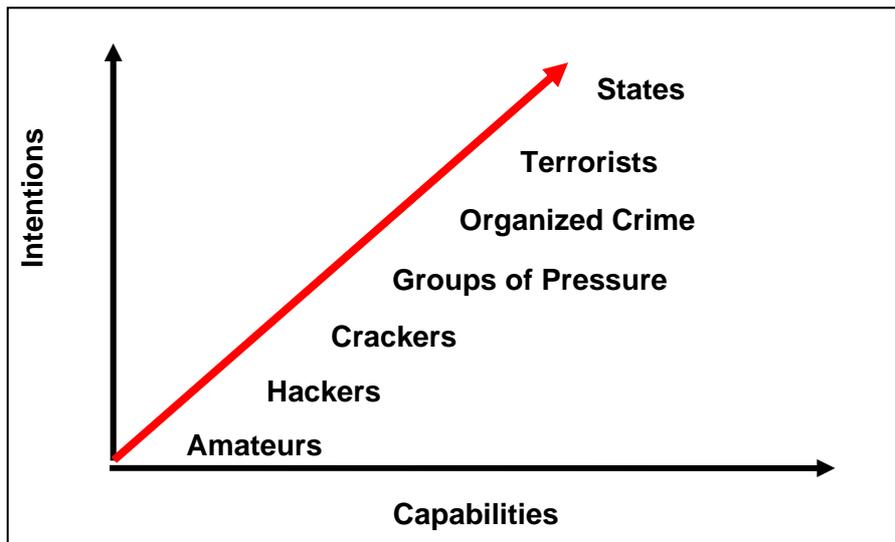


Figure 4 - National Information Infrastructures Threat Level

Attending to the Information Warfare nature and looking forward to explore its potential, many criminal groups and non-State actors can use information attacks to get illegitimate economical advantages¹³. Since information systems are increasingly used in financial transactions, it is natural to expect that different types of criminals will choose these systems as a target trying to profit and get important dividends from them.

The States' critical infrastructures dependence relatively to its information infrastructures makes them also attractive to terrorist groups. Terrorists may seek to launch information attacks (cyber attacks) with the objective to produce potentially disruptive effects in the critical infrastructures of the target State.

Information Warfare activities developed by competitor States constitute a significant threat that cannot be ignored in the context of this study. The aim or propose of these attacks will vary according to the objectives to reach, being able to assume the form of: isolated information attacks intended to influence the politics of other States, espionage activities trying to exploit the competitor States information domain (for economic, political or military purposes), countermeasures destined to cause the destruction of a specific Weapons System or a Command and Control System or, still, an attack focused on another State NII with the intention to cripple its vital infrastructures.

In this framework, it matters to distinguish a "strategic disruption" as the electric power 2003 blackout affecting Canada and the US from an "important" but not strategic disruption, such as the electric energy cut-off that also affected the United Kingdom and Italy some days later. As it can be proved through these examples, a "strategic disruption" presents a widened focus and a bigger temporal duration that will result in a superior disruptive power. If a State intends to launch an information attack with the objective of producing a "strategic disruption", at the precise moment that another State is conducting important activities for its survival, this will necessarily have a strategic effect that in some cases may conduct to the culmination of the target State.

In the current information environment, an information attack could thus be considered of strategic level if its impact will be so important that will affect (or come to affect) the

¹³ In this context, it can be stressed the fact that electronic payment systems (VISA, ATM, debit cards, etc.) are progressively replacing the traditional payment methods. It can be said that money is assuming more and more a digital form.

capability of a State to assure its vital functions (security and well-being of its population). Following this rationale and considering its effects, Information Warfare weapons, previously described, could be considered as weapons of "mass disruption" (Libicki, 1996; Morris, 1995), presenting its use a similar strategic framing to the one related to Weapons of Mass Destruction (WMD). Due to the uncertainty level of consequences and to the potential impact of Information Warfare attacks in the civil populations, the nation's information weapons strategy will have to be carefully planned and co-ordinated in its execution, by the highest level of its political hierarchy. Due to its direct implications in the National Strategy, the NII's defence and protection assumes a major role in the safeguard of national interests.

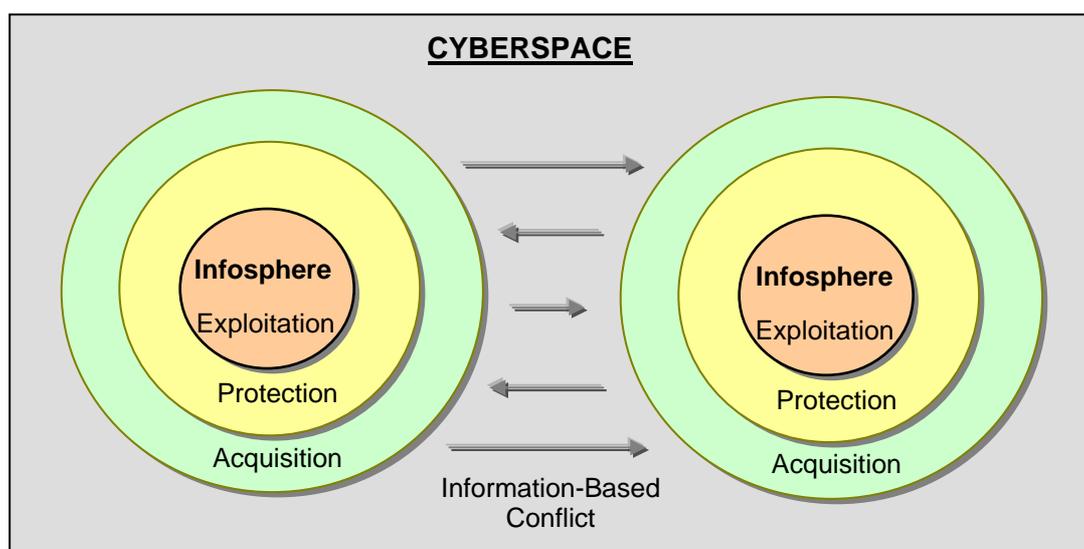
5. Implementing the National Information Strategy

Envisioning the implementation of the National Information Strategy in all its components is important to clarify its scope, the ends/purposes to be reached, its domains and the set of activities involved.

5.1. Scope

In contradiction with the information theory of Hartley Shannon, information does not only have to be used as a residual aspect in its context (Waltz, 1998). It participates in the context, making it to evolve. Besides that fact information is directly linked with the representations level and it cannot be distinguished from the action itself.

In the picture of modern conflict, the networks and information flows that support the decision and actions in the information domain must be established and followed in order to perceive and shape the reality. Only like this it will be possible to intervene on the information environment in order to influence its evolution according to the desired outcome.



Adapted from: Canadian Forces Information Manual Operations (1998)

Figure 5 - Information Use Scope

Information as a key-factor for the strategic level decision making can be represented as an "infosphere" (see Figure 5) that includes all the pieces of information collected from the diverse available sources. From this perspective, it will be possible to define a process of acquisition, protection and exploitation of the information (CFIO, 1998). The information acquisition constitutes the process through which our "infosphere" will look for to capture both friendly and potential adversaries' available information. The information protection represents the process that will allow us to defend and guarantee the security of this environment. Finally, the information exploitation constitutes the process through which the information is presented and integrated in the decision making process.

Hence, the National Information Strategy will have as scope the information-based conflicts that result from the competition and conflict relations generated between ours and other actor's infospheres.

5.2. Ends/Purposes

Taking into account the Information Strategy scope, we realise that it will be able to present three main ends/purposes, applicable to both civilian and military information environment:

- Information Assurance¹⁴ - one of the main challenges that Nations and their Armed Forces have to face in our days is the protection of its Information Infrastructure. This desideratum requires, as already mentioned before, as much the implementation of security mechanisms as the adoption of the appropriate information infrastructure defences. The existent specific knowledge in the information security area, the development of high survivability systems and the existence of a systemic and integrated process of risk analysis and risk management are considered elements of major importance to guarantee the Information Assurance.
- Information Superiority¹⁵ - After guaranteed the availability and the integrity of the State's information systems, a future option that could be considered is the expansion of the influence capability of its information environment (infosphere) towards other more widened environments, inside of which the organization or the State intends to intervene. To make this happen one organization should concentrate itself in the development of superior information systems guaranteeing its assurance and then induce potential adversaries to prematurely reveal its information environment defensive capabilities.
- Information Dominance¹⁶ - After friendly capabilities and information systems have established one definitive degree of information superiority, they will be in position to launch a campaign envisioned to obtain an operational advantage. The successful conduction of this campaign requires the dominance of the adversary's information environment by those that will need this information. To achieve information dominance in an adversary's information environment is mandatory that the friendly decision makers compromise themselves in creating the necessary conditions to launch a decisive information attack.

¹⁴ See JP 3-13 (1988, p.GL-7) definition.

¹⁵ See JP 3-13 (1988, p.GL-7) definition.

¹⁶ See FM 100-6 (1996, p.GL-7) definition.

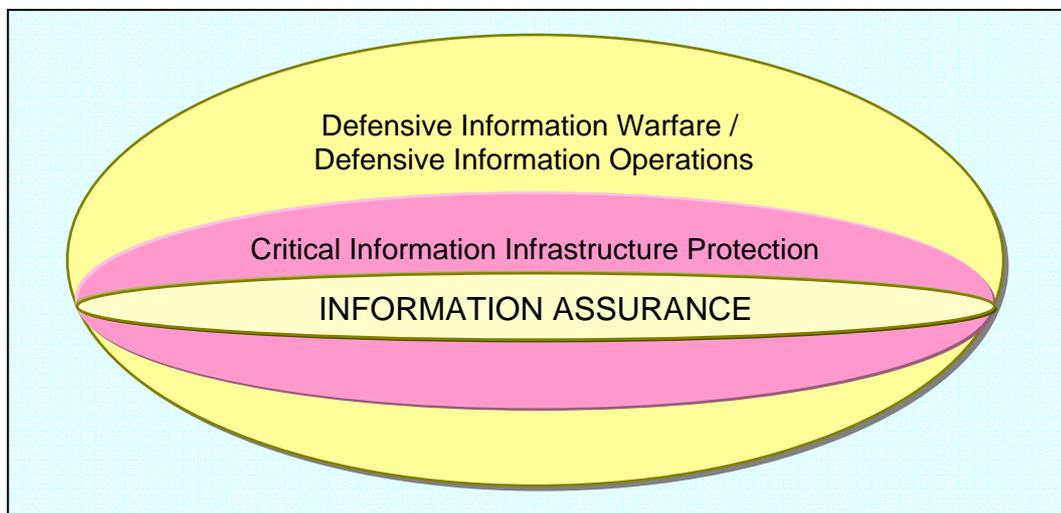
Every country, even the smaller ones, will have to take into account its national capabilities and will have to guide its Information Strategy in accordance with the national interests. A small country with modest capabilities in the information domain will have to establish as first priority the Information Assurance (1st phase) and to foresee the Information Superiority (2nd phase). We do not consider a realistic objective the development of the capabilities that are needed to achieve Information Dominance.

5.3. Competence Domains and Related Activities

The global information environment that integrates citizens, commercial organizations, governments, Armed Forces and even international organizations is interactive and permissive in its very nature and influence capability. Information became a resource of growing importance and extremely difficult to manage and protect. In a national perspective, this situation raises some major concerns namely:

- The availability and integrity of the information that supports high level political and military decision makers' decisions and actions;
- The country's efficiency in its information processing and exploitation of the available information-based systems.

Additionally we realise that the domains involved in the Information Strategy development, that will assure the NII's protection and defence, will be dependent upon national leaderships decision cycle, of the technical means used and of different arenas where actions take place (political, economical, psychological or military). Considering national strategy definition the identification of these elements is mandatory in order to guarantee the coherence of the responsibilities assignment. These are the competence domains.



Source: Lars Nicander (2001)

Figure 6 – National Information Infrastructure Protection Conceptual Model

Having defined the Information Assurance as the main end/purpose of the National Information Strategy (at least for a small country), we also need to identify the set of activities that will allow its fulfilment. Based upon the US doctrine and the Swedish reference model we are also tempted to consider that the National Information Security will only be achieved through the broader concept of Critical Information Infrastructure

Protection and that the Defensive Information Operations/Defensive Information Warfare activities performs a decisive role to assure that protection (see Figure 6).

Assuming that in the current strategic and economic environment a natural synergy between Information Warfare activities and Information Operations (INFO OPS) exists, we realise that at its implementation level National Information Strategy will have two fundamental components: Information Operations and the National Information Security.

Due to the specific nature of means and the different sectors (civilian and military) covered by the Information Strategy (see Figure 7), INFO OPS and Information security activities are conducted both in civilian and military arenas.

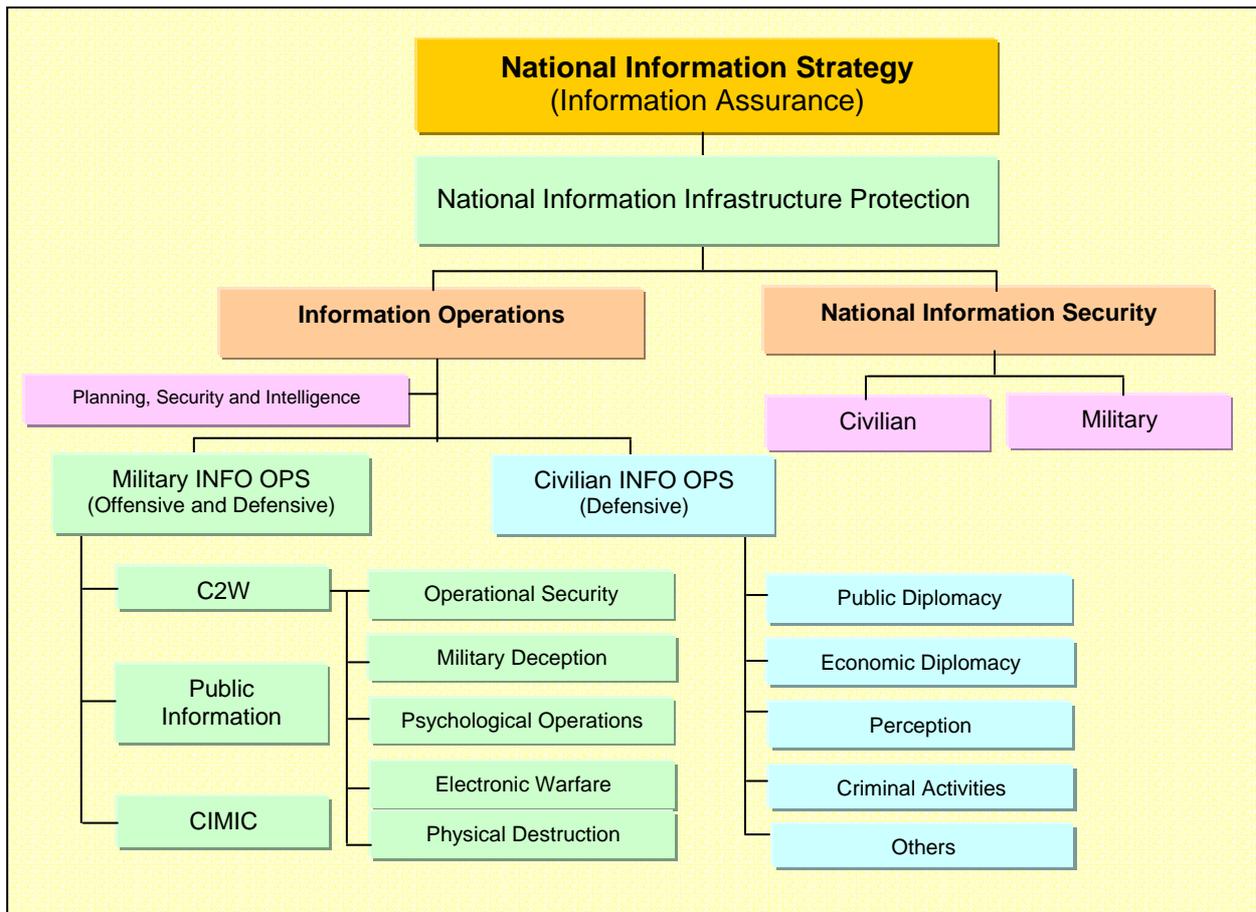


Figure 7 – Model for the Implementation of the National Information Strategy

The planning, security and intelligence activities assume an important role in INFO OPS success. This fact is better illustrated in the military arena but also reveals itself an important issue in the civilian arena.

6. National Information Infrastructure Protection

Knowing that the threat of Information Warfare completely eliminates the distinction between military and civilian systems, there still is the challenging question of knowing if any government can protect its own NII upon which it has neither the complete ownership nor control.

The need of a country to have a broad scope security and protection in the cyberspace domain is necessary to preserve the States capability to defend its national interests. A clear vision of this need will help to draw the path to be followed showing how to create a supporting structure to the implementation of a National Information Infrastructure Protection System (NIIPS).

In the implementation of such a system the rational to be followed will be the risk management approach: Protection, Detection and Reaction. Within this context the NII protection will involve the need to:

- Identify the information resources of national interest that can be attacked through the shared NII components;
- Define the procedures and the necessary mechanisms to assure the defence against the different kinds of NII threats;
- Implement an alert and report system that will allow to anticipate, detect and identify the attacks conducted against the NII and/or against the users of the information of national interest;
- Define the restrictions imposed by the threat spectrum and the adoption of possible responses, creating rules of engagement at both national and international level;
- Assure an external audit and the execution of permanent NII tests by means of specialized teams (*Red Teams*);
- Assure the existence of a Civilian and Military Corps of Information Specialists (“info-corps”) specially oriented to the security of information infrastructures and to the conduction of information Operations, since these areas will require special competencies;
- Identify the role that government and the private organizations have to perform in the creation, management and operation of systems linked to the Defensive Information Warfare capability and to the NII security.

In this context it is still necessary to assure an effective coordination of actions in both areas of information security and information operations. In this way it will be possible to avoid conflicts of interests and stimulate the cooperation both in national and international arenas, clarifying the distinction between law enforcement and national security problems.

The organizational solution to this problem will have to include the creation of specific laws that assure the difficult equilibrium between individual wrights and institutional responsibilities. These legal aspects will allow the clarification of the objective, attributions and competencies of all the entities of NIIPS structure.

Conclusions

Cyberspace as a space where national interests are defended imposes new interaction and relationship patterns between political actors. The strategies used in this domain are centred in the value of the information resources and in the operations conducted to affect that value.

Although complex in its design and planning we cannot ignore the need of a National Information Strategy. If such a strategy wouldn't exist, in the context of the international relations, any country will incur the risk of being pushed to a position of simple follower of

strategies dictated by powerful nations or organizations that conduct Information warfare activities in this domain.

The definition of a National Information Strategy will only make sense if we also envisioned an organizational structure and its related capabilities. Its implementation will also demand the definition of its operational (related with the use of resources), genetic (related with the generation of new resources) and structural aspects (related with the organization and articulation of these means).

We conclude that there is a need for extraordinary action to deal with the present and emerging challenges of defending against possible information attacks on National Critical Information Infrastructures, which would seriously affect the ability of national authorities to carry out its assigned missions and functions. Accordingly, we recommend a series of actions designated to better prepare a Nation State for this new form of information-based warfare (Information Warfare).

The perception that the existent mechanisms and security processes have difficulties to follow the dynamics of vulnerabilities, raises the urgent need of a strong national campaign in order to capture the attention to the importance of defending and protecting the national information infrastructures and resources. This will force the Nation States to review the current national security and defence concepts.

REFERENCES

Books and Manuals:

- ARQUILLA, John et al (2001). *Networks and Netwars: The Future of Terror, Crime, and Militancy*, National Defense Research Institute – RAND.
- CAMPEN, Alan et al (2000). *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict*, AFCEA International Press.
- CARDOSO, Sousa (2003). “Guerra no Ciberespaço: Um Novo Método de Conflito”, Conferência proferida na Academia Militar ao Curso de Pós-Graduação em Guerra de Informação/Competitive Intelligence (não publicada), 26 de Julho.
- CASTELLS, Manuel (1999). *A Sociedade em Rede*. São Paulo, Paz e Terra.
- CFIO, (1998). *Canadian Forces Information Operations Manual*, Documento Doutrinário do Estado Maior de Defesa do Canadá, B-GG-005-004/AF-010, 14 de Abril.
- COUTO, Cabral (1988). *Elementos de Estratégia*, Volume I, IAEM.
- DENNING, Daniel (2000). *Activism, Hacktivism and Cyberterrorism: The Internet as Tool for Influencing Foreign Policy*, Nautilus Institute.
- DMDM, (2002). *Directiva Ministerial de Defesa Militar*, MDN, Janeiro.
- ERBSCHLOE, M. (2001). *Information Warfare: How to Survive to Cyber Attacks*, McGraw-Hill.
- LIBICKI, Martin (1995). *What is Information Warfare?*, National Defense University Press, Washington D.C.
- NICANDER, Lars, (2001). “*Information Operations/Critical Infrastructure - A Swedish View*”, Comunicação proferida pelo Director for National Office of IO/CIP Studies no Swedish National Defence College no Seminário “InfoWarCon 2001”, Apresentações da Conferência.
- RAMALHO, Pinto (2003). “A Direcção Geral de Política de Defesa Nacional”, Conferência proferida no Instituto de Altos Estudos Militares ao Curso de Estado-Maior (não publicada), 24 de Junho.
- TABORDA, João et al (2002). *Competitive Intelligence*, Editora Pergaminho Lda., Cascais.
- WALTZ, E. (1998). *Information Warfare: Principles and Operations*, Artech House.

Reviews and Other Periodic Publications:

- CAETANO, Paulo e GARCIA, Rita (2003). “Portugueses em Perigo”, in *Revista FOCUS*, 27 de Agosto, pp.96-100.
- HERZFELD, Charles (1999). “The Defence of Infrastructure”, in *Information Impacts Magazine*, Setembro.
- LEWIS, James (2002). “Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats”, Artigo do *Center for Strategic and International Studies (CSIS)*, Washington D.C., Dezembro.
- LUKASIK, Stephen (1999), “Defending Information-Dependent Infrastructures”, in *Information Impacts Magazine*, Setembro.

Sites and Web Pages:

- ANDERSON, R. et al., (1999). *Securing the U.S. Defense Information Infrastructure: A Proposed Approach*, RAND Technical Report, in <http://www.rand.org/publications/MR/MR993>.
- COHEN, Fred, (1999). *Strategic Security Intelligence: Information Warfare*, Fred Cohen & Associates, in <http://all.net/index.html>.

- COHEN, Fred, (1999). *Strategic Security Intelligence: Information Warfare*, Fred Cohen & Associates, in <http://all.net/index.html>.
- COM, (2002). Comunicação da Comissão ao Conselho, Parlamento Europeu, Comité Económico e Social e Comité das Regiões, *e-Europe 2005: Uma Sociedade da Informação para todos*, Comissão das Comunidades Europeias, (COM 2002) 263 Final, Bruxelas, http://europa.eu.int/information_society/eeurope/news_library/eeurope2005/index_en.htm.
- FM 100-6, (1996). *Information Operations*, in <http://www.jya.com/fm100/fm100-6.htm>.
- FRANCART, Loup, (2000). *La Maitrise de l'Information*, in www.infoguerre.com.
- JP 3-13, (1998). *Joint Doctrine for Information Operations Publication*, Joint Chiefs of Staff, Joint Electronic Library, in http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf.
- KUSCHNER, K. (2002). *Legal and Practical Constraints on Information Warfare*, in <http://www.airpower.maxwell.af.mil/airchronicles/cc/Kuschner.html>.
- LUIJF, Ir. et al (2003). *In Bits and Pieces*, in INFODROME, <http://www.infodrome.nl/>.
- MORRIS, Chris et al., (1995). *Weapons of Mass Protection: Nonlethality, Information Warfare, and Airpower in the Age of Chaos*, *Airpower Journal*, in <http://www.cdsar.af.mil/air-chronicles.html>.
- NSHS, (2002). *National Strategy for Homeland Security*, in White House Office of Homeland Security, http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf.
- NSSC, (2003). *National Strategy to Secure Cyberspace , Definição da Estratégia Nacional de Segurança do Ciberespaço dos Estados Unidos da América*, in White House Office of Homeland Security, http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf.