Security of Critical Information Infrastructures: E-Governance and Standardization

Serap Atay, Marcelo Masera

Abstract— **Critical Information Infrastructure - CII is a key enabler of e-Governance. This infrastructure is composed of the Information and Communication Technologies –ICT- underpinning the higher level services to end users, and encompasses the Internet, fixed and mobile telecommunications and other systems. The gap between security solutions and security risks is continuously growing due to evolution of the ICT. Each new technology and application can include many flaws. Each flaw may pave the way to unauthorized users to accessing critical data and/or may mistakenly provide them with the ability to perform some harmful action. Nowadays, the CII is in a conversion phase towards the so-called Next Generation Networks – NGNs. With this development, all telecommunication services will be built upon IP based networks. Naturally, these developments force the standardization bodies to adapt their rules and policies and thus to meet the security needs of these new CII components. E-government services such as administration, health, education etc. either create new services or replace existing manual procedural systems. These new services should offer higher availability, security and reliability with respect to current operations due to their increasing criticality. This criticality should be managed in innovative e-Governance arrangements among public and private actors: mainly the authorities and the operators of the CII, but also including all relevant stakeholders. In the meantime, the governments should be prepared for this new paradigm of e-Governance. The aim of this paper is to summarize the benefits and security risks of NGNs and emphasize the basis and requirements for that e-Governance.**

***Index Terms*— Communication system security, Government information systems, Internet, Security.**

I. Introduction

The aim of this paper is to define the importance of Critical Information Infrastructure – CII and the developments of NGNs for the availability, security, and reliability of the e-governance services.

First of all, the difference between e-government and e-governance should be explained. E-government refers to the use of Internet technologies for expediting the links of the government (executive, legislative, judiciary, local administration) with citizens and the private sector. It integrates the interactions and the interrelations between and among government and citizens, companies, customers, and public intuitions through the application of modern information and communication technologies. E-governance refers to the process of using information technology for facilitating the joint operations of government, nonprofit, and private-sector entities, as well as the interactions with citizens, other authorities and organizations [1]. The main distinction is that in E-Governance all participants are part of a network, while in E-Government the main actor is the government.

E-governance is understood as a powerful tool to overcome existing barriers for development of countries with the following properties;

- automation and citizen centric service delivery,
- accessing to these services from anywhere and anytime,
- increasing accountability and
- in order to achieve much more citizen participation.

Therefore, e-governance can be accepted as a new culture for governments for dealing with problems where the actors are multiple and where the government is not the only, privileged participant.

E-governance services create new services or replaces manual procedural systems for aforementioned objectives. For the usability of e-governance services, the confidentiality, integrity, authentication, non-repudiation, availability, reliability, responsiveness and assurance should also be created. Also, these properties should be supported by laws.

The governments tend to maintain e-governance services for many critical infrastructures - CI such as transportation, water, energy, finance, justice, health etc. However, all these CIs use another common critical infrastructure which is called as Critical Information Infrastructure – CII. Consequently, these infrastructures are interrelated or interdependent through CII. Therefore, the Critical Information Infrastructure Protection – CIIP is so important for the governments. The Fig. 1 depicts these relations.

Manuscript received November 10, 2008. This work was supported in part by the TUBITAK (Turkish Science and Technological Research Program) under Grant of Bideb2219 Post-Doctorate Research Fellowship.

S. ATAY, Author is with the Institute for the Protection and the Security of the Citizen, Joint Research Center, Via E. Fermi, 21020, Ispra, Italy (e-mail: serap.atay@jrc.it) and Izmir Institute of Technology, Department of Computer Engineering, Izmir, Turkey (mail: serapatay@iyte.edu.tr).

M.MASERA, Autor is with the Institute for the Protection and the Security of the Citizen, Joint Research Center, Via E. Fermi, 21020, Ispra, Italy (e-mail: marcelo.masera@ec.europa.eu)

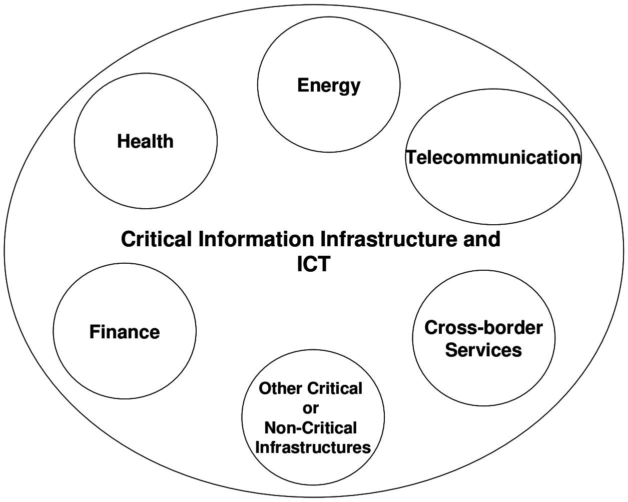
Energy
Health
Telecommunication
Critical Information Infrastructure and ICT
Finance
Cross-border Services
Other Critical or Non-Critical Infrastructures

Fig. 1. The critical and non-critical infrastructures have an information infrastructure which uses the common information and communication technologies.

CII can be easily affected by the any changing or development of Information and Communication technologies such as communication, hardware or software technologies. In the mean time these technologies are very fast changing and improving. These improvements, changes and new interconnections between infrastructures may be causes new vulnerabilities, threats or attacks through directly or indirectly.

According to survey report is prepared by Secure Computing; 'when asked about the interconnection of control networks and corporate networks, over 60% of the Secure Computing survey respondents said their networks were already interconnected and 98% said that interconnection increased their security risks'[1]. Survey data of this report had collected from attendees at the Process Control Systems Industry Conference held August 26-28, 2008 in La Jolla, California; attendees at the 1st Annual Cyber Security Conference held September 8-9 in Calgary, Alberta; and an online survey of critical infrastructure cybersecurity experts in Europe, the Middle East, and Africa during September 10-25, 2008. A total of 199 respondents had completed the survey.

Additionally U.S. Department of defence -DoD reported the number of incidents of malicious cyber attacks in May 20, 2008. As shown from the Fig. 2 the rate of attacks is increasing %31 between 2006 and 2007.

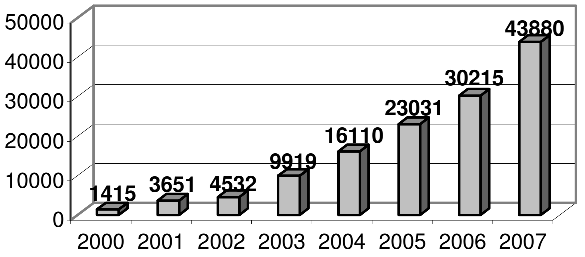

Fig. 2. U.S. Department of Defence (DoD) Reported Incidents of Malicious Cyber Activity [14].

Nowadays, the telecommunication infrastructure is in a conversion phase for the Next Generation Networks – NGNs. Naturally, these developments will come with lots of unknown vulnerabilities, threats, and security risks.

According to aforementioned reports and the definition of the high consequence risks facing the UK in the report of Centre for the Protection of National Infrastructure – CPNI [13]; the interconnectivity among networks is expanding and the probabilities and impacts of attacks with NGN reach higher values as illustrated in Fig. 3.

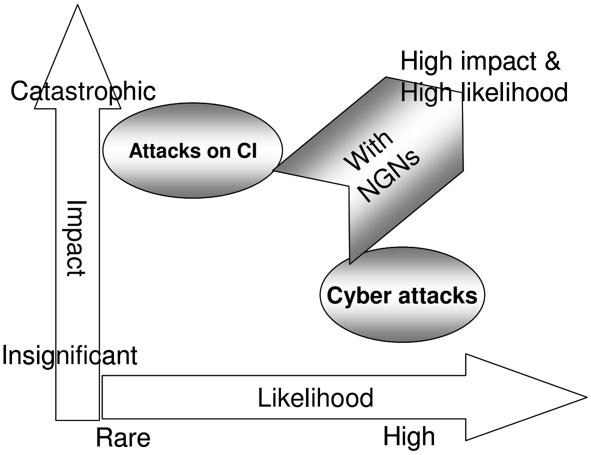

Fig. 3 An illustration of the high consequence risks with NGNs.acing

This situation forces the research institutes and standardization bodies adapt their rules and policies to meet the security needs of the new CII. Currently, the governments are planning to improve the ICT and the e-governance services and for that, they should do some preparations for the security of e-governance and NGNs.

This paper is organized with the following sections; the section 2 includes information about the NGNs and their benefits for the e-governance and CII. The section 3 defines the security risks of CII and e-governance services. The section 4 defines the standardization studies for NGNs. Section 5 concentrates on the definitions of requirements of e-governance and security with a proposed solution list. Section 6 presents the conclusions of this study.

[1] Critical Infrastructure Cybersecurity: Survey Findings and Analysis Whitepaper Sponsored by: Secure Computing, Rick Nicholson, November 2008.

II. NEXT GENERATION NETWORKS AND BENEFITS OF E-GOVERNANCE

The requirement of ICT is growing for e-governance, global market, industry, education, health and multimedia services etc. These requirements expand the digital traffic and costs. Therefore, the telecommunication sector has a plan about the convergence and optimization of traditional networks.

The aim of telecommunication sector with the NGN is collection of existing networks (such as fixed, mobile, broadcast, data, internet etc.) into unitary network architecture. This new architecture is to be a packet-based network and will be using multiple broadband technologies. As shown in Fig. 4. the idea of NGN is to have an infrastructure a reusable and services centralized and avoid discrete networks overlaid on existing network for each new service.

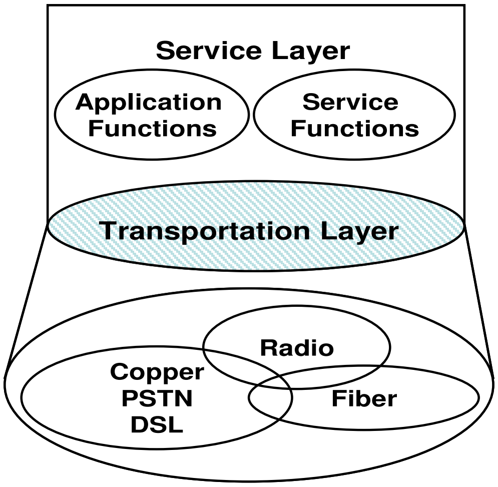

Fig. 4. NGNs transform communication technologies to service-centric unitary network architecture.

NGN are being developed by using a number of different technologies, including wireless and mobile, fiber and cable, or by upgrades to existing copper lines. The service-related functions in NGNs are independent of transport technologies when providing telecommunication services to users. So, from a more technical point of view, NGN is defined by the International Telecommunication Union–ITU as a "packet based network able to provide services including telecommunication services and able to make use of multiple broadband, quality of service - QoS enabled transport technologies and in which service related functions are independent from underlying transport-related technologies."[2]

According to ITU report "Trends in Telecommunication Reform: the Road to NGN" published in September 2007, it is predicted that full implementation of NGN in fixed line networks in developed countries will be deployed by 2012 and in mobile networks by 2020. Developing countries are also seeking to deploy NGN technology, although not necessarily following the same path as developed countries [3].

Benefits of NGNs for e-Governance

One of the objectives of the NGN is to establish higher quality communication infrastructure for everyone and from everywhere.

- The ICT supports all economic sectors, is crucial to the national and international exchange of goods and services and economic interrelationships through related services. As a result, it has become a key economic and social infrastructure for all countries and citizens with this property.

The unitary and completely IP based infrastructure will decrease usage costs for the communication infrastructure. But, first investments of NGN and NGN access are high for the operators [4]. The aim of the NGNs is to have an access for every place with higher bandwidth.

- In this case, the e-governance services can be reachable from the rural places. This property helps to the availability of e-governance services.
- High speed networks with NGN will increasingly help to resolve ongoing social concerns in areas such as the environment, healthcare, education and are increasingly playing a role in social networking (facebook etc.).

In the mean time, this innovative technology is expected to bring about greater energy efficiency than legacy networks. By improving the energy efficiency of Information and Communication Technologies (ICTs), NGN can potentially make a significant contribution in the battle against global warming [3].

III. THE SECURITY RISKS OF CII AND E-GOVERNANCE

The formal definition of Critical Infrastructure-CI for the European Countries is 'critical infrastructures which disruption or destruction would significantly affect two or more Member States or a single Member State if the critical infrastructure is located in another Member State"[3]. Now, this includes effects resulting from cross-sector dependencies on other types of infrastructure therefore for the potential of NGNs, some services required closed to the national or universal coverage.

The Supervisory Control and Data Acquisition – SCADA networks can be taken as a good example to show the risks. The system monitoring, control, and status data gathering in most CI are now automated processes with reduced reliance on human effort. These processes rely on SCADA networks and these are closed networks. So security was not addressed in great depth compared to conventional ICT systems. Unfortunately, today many corporate network and their leased lines are parts of SCADA network. These parts provide direct or indirect connectivity points to the internet and other networks. So, many examples exist about security vulnerabilities of SCADA network. For instance; in January 2003 the Slammer worm disrupted SCADA traffic causing operators to temporarily lose some degree of control of the

[2] ITU-T Recommendation Y.2001, approved in December 2004, available at http://www.itu.int/ITU-T/studygroups/com13/past-results.html

[3] European Commission 2006a, p. 15

Davis-Besse nuclear power plant in Ohio USA. As a result, there is now increased acknowledgment of the possibility of external attacks on SCADA networks by CI owners and notable surge in interest in SCADA systems by terrorist groups.[4]

The physical cross-borders between governments are removed by ICT. Many e-governance services will be deployed over national borders. See for instance the offer of e-health to international tourists. Interconnection across borders means that attacks can come from anywhere and anytime, infiltrating the public (governmental) and private sections of the CII. This risk is coming from 'multi-party cross-border' relations of the governments and the risks become to have unpredictable dimensions with NGNs. The Fig. 5 depicts the multi-party cross-border relation for the security risks. This highlights the need for developing international approaches for the protection of the CII, and the prevention and management of related incidents.

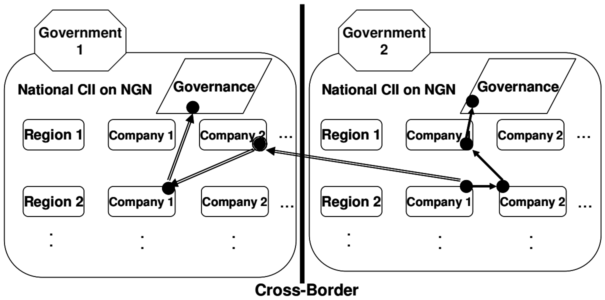

Fig. 5. NGNs have unique communication infrastructure and its affect on national CIIs is 'multi-party cross-border'.

Each new ICT technology inevitably includes new vulnerabilities. Threats are either to exploit these vulnerabilities directly or indirectly to create an attack. Therefore, many vulnerability, threat and risk analysis should be done for NGNs – and these should also include infrastructures and multy-party situations. Typical ICT security assessment approaches do not contemplate these situations, and new methodologies are needed. The most important part of this process is that the results of these analyses should be employed for reshaping the related security standards and common criteria.

IV. Standardization Studies for NGNs

Standardization is a consensus-driven activity and an important mean for achieving and establishing trust between the parties involved. It is based on openness and transparency within independent organizations. Some of the important objectives of standardization are the establishment of compatibility and interoperability, the removal of barriers through harmonization, and the safety and health of citizens. As a consequence, the three groups of stakeholders primarily benefiting from standardization processes are industry, consumers and governments.

Telecommunication services are created on IP networks in NGNs. This creates a demand on standardization bodies to adapt and meet the needs of these emerging networks. The goal is to develop specifications that are ready for an assurance audit and, using the common criteria for security evaluation as well [7]. International Standard Development Organizations - SDOs such as ITU, ETSI, ISO, IETF, and 2GPP/3GPP2 are working to integrate security into the definition of NGN standards and protocols, in order to appropriately address security in the design phase of the new generation of networks.

ITU has ITU Global Cybersecurity Agenda – GCA which is an ITU framework for international cooperation aimed at proposing strategies for solutions to enhance confidence and security in the information society. It will build on existing national and regional initiatives to avoid duplication of work and encourage collaboration amongst all relevant partners.

At ITU-T, the international standardization of NGNs is underway as part of the NGN Global Standards Initiative[5] - NGN-GSI, involving various standards organizations. The NGN-GSI focuses on developing the detailed standards necessary for NGN deployment so that service providers can offer the wide range of services expected from NGN.

ETSI TISPAN (Telecommunications and Internet converged Services and Protocols for Advanced Networking) has been the key standardization body in creating the NGN specifications since its creation in 2003. NGN Release #1 was finalized in December 2005, provided the robust and open standards that industry required for the development, testing and implementation of the first generation of NGN systems. NGN Release #2 was finalized in early 2008, and added key element to the NGN such as IP Multimedia Subsystem - IMS and non IMS based IPTV, Home Networks and devices, as well as NGN interconnect with Corporate Networks.

A major part of any security specification and of a security product is the measure of assurance it provides with respect to the security it offers. The Common Criteria as identified in ISO/IEC 15408. This is the best known tool for evaluation of security [6].

V. Requirements of E-Governance Services and Security

This section discusses the definition of security requirements for e-governance. Firstly the objectives of the governments, other related service providers and the expectations of the end users should be clearly defined. The e-governance services may cover the many type of users such as; from inside of the government, civilization (from cities, rural areas or from other countries), military forces, justice departments, national security units and some services from other governments etc.

The services of e-governance and its requirements have to

[4] Critical Infrastructure Protection in the Baltic Sea Regions, chapter 3, 2007.

[5] http://www.itu.int/ITU-T/ngn/

establish the availability, reliability and privacy from the point of view of the users, which can be classified according to different categories. Therefore,

- The security standards and policies are to be used by the all involved parties in the governments and industry. As presented in section 1, all critical and non-critical information infrastructures use the common CII.
- The governments should have incident response systems and policies for the emergency cases. Private actors should be involved, always in respect of business confidentiality and fair market rules. Specific e-Governance arrangements for security should be put in place.
- The public and private suppliers and users of e-government and e-governance services should be aware about the related security risks. The training for everybody is important requirement for the security, reliability and availability of e-governance services.
- The governments are doing investments to build e-governance services and its technological infrastructure, so the usage rates of these services are very important. To improve the usage rates, the training of the end users is an important aspect. Education system and methods should be evaluated for all level from first school to universities and for the public by the government. Dedicated e-Inclusion policies (for the elders, people with temporary or permanent disabilities, etc.) should be studied.
- ICT will give important possibilities to access all people to educate them. All citizens should be empowered from the functional and security viewpoints. Education can and should continue for the whole life-span of the people.

The security professionals, research and accreditation centers, service companies and organizations are necessary for the secure systems design, detection of vulnerabilities, threats and risks. For this objective;

- The universities and their departments and curriculums should be evaluated and updated. Security studies should be recognized as a key component of all relevant curricula – and not only the particular computer science department.
- Global research activities about ICT should be closely followed. The specific organizations, research centers and universities should join to global standardization organizations and follow the developments; since the earlier experiences are so valuable at the beginning of transformation to NGNs infrastructure and e-governance.
    - There are some early NGN implementations in UK and Japon. Their early NGN implementations -including field trials- were established in 2006 such incumbent operators as BT in the UK, NTT in Japan, and AT&T in the US. By the end of 2008, NTT expects to offer complete NGN services on a full scale, and BT has announced that it expects half of its customer base to have migrated by 2008, and the migration to be "substantially complete" by the end of the decade[3].
- To use the same internationally approved terminology, concepts and security standards are other important facilitators of the e-governance.

The governments should reorganize the civil and governmental policies and should update the laws to support e-governance services and establish the security requirements as harmonized with inside and outside of the government regulations. So, the governments should sign all relevant international agreements for tracing criminals, and cyber warriors across borders.

VI. Conclusions

Standards and common criteria agreed at the international level should be accepted and be used globally in a harmonized structure. This requires a change in mentality in governments; since they have their own national traditions, institutional structures, policies and strategies, vocabulary, technical and methodological approaches.

In addition, e-governance requires the close interaction of public and private actors, and a shared approach to security. In an e-governance setting, governments had to take into consideration the opinions, concerns and positions of private actors. In the field of NGN, the security of the resulting critical infrastructure will depend on the convergence of positions among public and private actors.

Typically countries prefer not to publish their research results about vulnerabilities and threats as they might affect their national security, but to detect all vulnerabilities and threats is impossible for each individual country. Therefore, there is the need to develop the right arrangements for sharing their experiences in a global environment. The sharing of these information and usage should be regulated by international agreements and rules.

The CII security problem will never be solved completely, because the nature of the problem is NP-complete [8]. The governments therefore should:

1. Recognise that the security problem should be approached by complementing the best available science and technology with heuristic methods, as it is a NP-complete problem. So, as Einstein said that “The significant problems we have cannot be solved at the same level of thinking with which we created them”, then we will do much more research on the problem with the new technologies which will have the heuristic abilities except Turing computational model.
2. Recognise that the security of CII and e-governance needs urgent solutions. The governments should support standardization research, other security-related research, and security education. New regulations,

standards should be created to force minimal level security goals for all ICT solutions. And, the governments should have an action plan and should do some investments to establish the requirements which are presented in section 5.

Acknowledgment

Thanks for the support of Assoc. Prof. Koltuksuz, A., Ph.D. from Institute of Technology Department of Computer Engineering, Turkey.

References

[1] G.Narayan, A.N.Nerurkar, “Value-proposition of e-governance services” International Journal of Education and Development using Information and Communication Technology (IJEDICT), 2006, Vol. 2, Issue 3, pp. 33-44.

[2] ITU-T Recommendation Y.2001, approved in December 2004, available at http://www.itu.int/rec/T-RECY 2001-200412-I/en.

[3] Next-Generation Networks and Energy Efficiency, ITU-T Technology Watch Briefing Report Series, No. 7, Agust 2008.

[4] “Next-Generation Network Architecture: What and When?”, Analysys Mason Group, Jan 2008, http://www.researchandmarkets.com/reports/c82216.

[5] International Standards Organization. ISO/IEC 18045, Information Technology – Security techniques – Evaluation criteria for IT security, 2005.

[6] S. Cadzow, “Securitv assurance and standards - design for evaluation”, Secure Mobile Communications Forum: Exploring the Technical Challenges in Secure GSM and WLAN, 2004. The 2nd IEE (Ref. No. 2004/10660) Volume, Issue , 23 Sept. 2004 Page(s): 8/1 - 8/6

[7] International Standards Organization. ISO/IEC 18045, Information Technology – Security techniques – Evaluation criteria for IT security, 2005.

[8] N.Li, Q.Wang, “Beyond Separation of Duty: An Algebra for Specifying High-Level Security Policies”, Journal of the ACM, vol. 55, No 3, article 12, July 2008.

[9] M.Masera, I.N.Fovino, R.Sgnaolin, “A Framework for the Security Assesment of Remote Control Applications of Critical Infrastructure”, 2005.

[10] E. P. Rathgeb, A.Krupp, H.Chair, “Dependable communication – vision or illusion?”,Proceedings of the 32nd EUROMICRO Conference on Software Engineering and Advanced Applications, 2006.

[11] P.Stuckmann, R.Zimmermann, “Towards Ubiquitous and Unlimited-capacity Communication Networks- European Research in FP7”, Eurepean Commission, 2007.

[12] “Trends in Telecommunication Reform 2007 The road to Next-Generation Networks (NGN), Summary”, ITU Publication, September 2007.

[13] National Risk Register of UK government, last updated 09 Nov. 2008 http://www.cabinetoffice.gov.uk/media/cabinetoffice/corp/assets/publications/reports/national_risk_register/national_risk_register_introduction.pdf

[14] U.S. e– China Economic and Security Review Commission, Hearing on China’s Proliferation Practices, and the Development of its Cyber and Space Warfare Capabilities, testimony of Colonel Gary McAlum, Washington, DC, May 20, 2008.

S. ATAY (M’02) She was born in 1966, received her BS in Computer Engineering from Ege University, Turkey in 1987 with a thesis on Expert Systems. Obtained her Ms.E from the same institution in 1989 with a thesis of a Systems Analysis and Design of Arkas Holding Information Systems. She worked in Arkas Holding as an Information Systems Coordinator in between 1987-2002 and conducted many projects concerning the maritime, air, rail transportation, port management and logistics. She started her academic life in 2002 and completed Ph.D. research on Information Systems Security and Cryptology in Information Systems Strategy and Security Lab. of Izmir Institute of Technology, Turkey concerning the “Computational Speed Problem of Elliptic Curve Cryptosystems in Software Implementation”. She has been doing post doctoral research on Security of Next Generation Networks project in Institute for the Protection and the Security of Citizen, Joint Research Center, Italy with support of postdoctoral research fellowship program of TUBITAK, Turkey since September 2008.

M. MASERA Born 22 September 1956. He has a degree in Electronics & Electrical Engineering (1980). Since November 2000 he is a scientific officer of the European Commission at the Joint Research Centre (Ispra, Italy).

He is in charge of the “Security of Critical Networked Infrastructures” area within the Institute for the Security and Protection of the Citizen. His interests are on the dependability and security of complex socio-technical systems, and specifically those related to critical infrastructures, large-scale systems-of-systems, information and communication technologies and the information society.

He has been researcher in the areas of Risk and Reliability at the National Research Council of Argentina (1981-1989), and visiting scientist at the JRC in the 1990- 1992 and 1997-1998. During these periods he has participated in the organization of the European Dependability Initiative, related to the Information Society Technologies R&D programme of the European Commission, and participated in several international projects.

He has been an independent consultant in the field of dependability of information systems (1992-1997), mainly supporting R&D activities and taking part in national and international projects.

He has published more than 60 papers in the fields of dependability, security and risk.