



Giornata di Studio
**La sicurezza dei cittadini
nelle aree metropolitane**



Perchè un Master in Homeland Security

Prof. Roberto Setola

Università Campus Bio-Medico di Roma

r.setola@unicampus.it

Roma, 25 Ottobre 2010

Sala Conferenze, PRABB Università Campus Bio-Medico, Roma

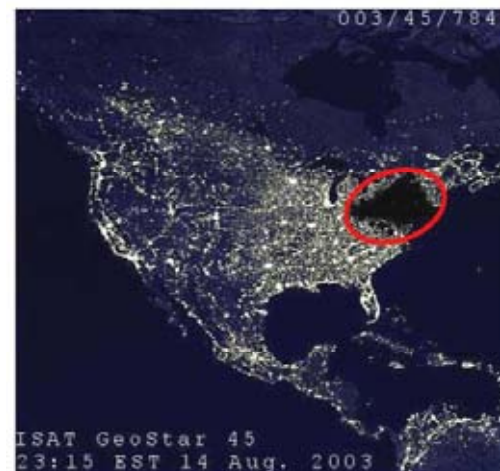
La società moderna richiede maggiore “sicurezza”



Catastrofi naturali



Consapevolezza



Criminalità



Terrorismo

Sicurezza

Evoluzione delle minacce

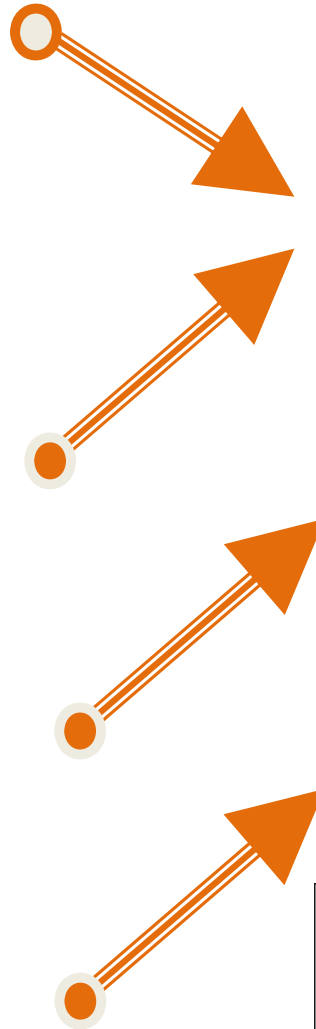
Eventi estremi

Guasti

Eventi naturali

Eventi complessi

Azioni dolose



Government of Canada / Gouvernement du Canada

Office of Critical Infrastructure Protection and Emergency Preparedness

Bureau de la protection des infrastructures essentielles et de la protection civile



THREAT ANALYSIS

Number: TA03-001
Date: 12 March 2003

Threats to Canada's Critical Infrastructure

Purpose

The purpose of this paper on *Threats to Canada's Critical Infrastructure* is to provide a taxonomy of the **natural**, **accidental** and **malicious** threats that have been identified as those most likely to impact upon Canada's national critical infrastructure. The paper will aim to provide informed forecasting for the relative probability of these threats and hazards.

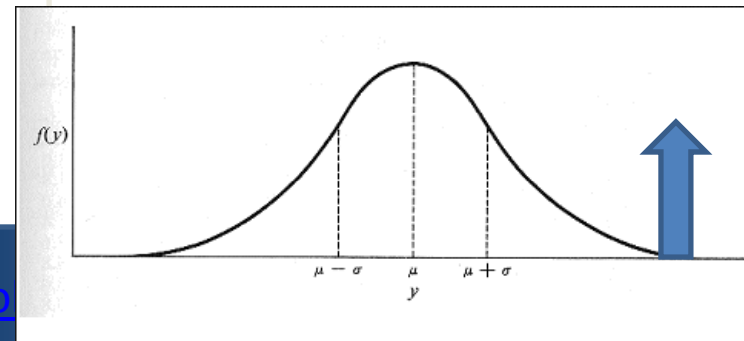
Audience

This report is primarily intended to provide owners and operators of Canadian critical infrastructure (CI) with baseline information regarding potential threats to their networks and systems. Owners and operators are the acknowledged experts with regard to the vulnerabilities they confront, but many have indicated that there is a lack of credible information regarding threats.

Emergency managers in the public and private sectors could also employ this report to enhance their understanding of the variety of threats and hazards which the Government of Canada is addressing.

Finally, policy makers at all levels of government may use the paper as a jumping-off point to examine threats and vulnerabilities in CI sectors within their constituencies.

Note: For the purposes of this paper the terms "**threats**" and "**hazards**" will be used interchangeably to describe the independent variables which affect existing vulnerabilities to produce risk/disaster scenarios.



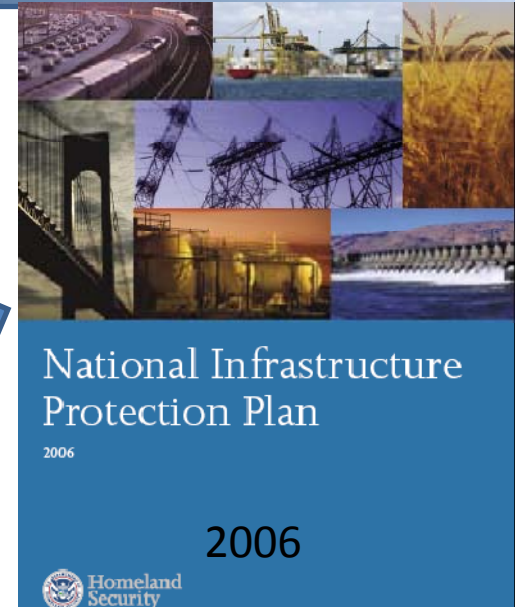
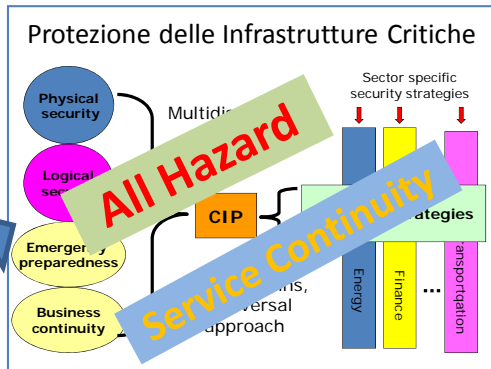
Critical Infrastructure Protection



Direttiva Europea 2008/114/EC

on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

Entrata in vigore il
12 Gennaio 2009



Direct terrorist attacks and natural, manmade, or technological hazards could produce catastrophic losses Attacks using components of CI/KR as weapons could have even more devastating physical and psychological consequences

Urban Control

Video Sorveglianza Urbana

25 million Closed-Circuit Television (CCTV) cameras worldwide

15.000 cameras are connected in the Chicago surveillance system (with a 30% crime reduction from 2006)

4.2 million CCTV in UK (1 for every 14 residents)

But they were unable to avoid the London terrorist attack !!!



Master in Homeland Security

III Edizione, Master di II livello (a.a. 2010-11)

Master in Homeland Security

Sistemi, metodi e strumenti per la security ed il
crisis management

Finalità

formare professionisti in grado di supportare il processo di analisi delle esigenze di sicurezza, di identificare le contromisure da adottare, di progettare e sviluppare soluzioni integrate e, per ciò che riguarda l'attuazione, la gestione e l'esercizio di procedure e di sistemi di sicurezza.

Destinatari

coloro che aspirano a lavorare come progettisti di sistemi e soluzioni di sicurezza all'interno di aziende pubbliche e private, ovvero figure professionali o consulenziali di enti e aziende con responsabilità nella gestione di Infrastrutture Critiche, di Protezione Civile, di Sicurezza, Difesa e Controllo del Territorio (Regioni, Comuni, ecc.).

III ed. Master in Homeland Security - partner



Enti organizzatori



a.a. 2010-11



Soggetti Partner



Con il contributo dell' Arma dei Carabinieri

Master in Homeland Security – Consiglio Scientifico

Direttore Scientifico

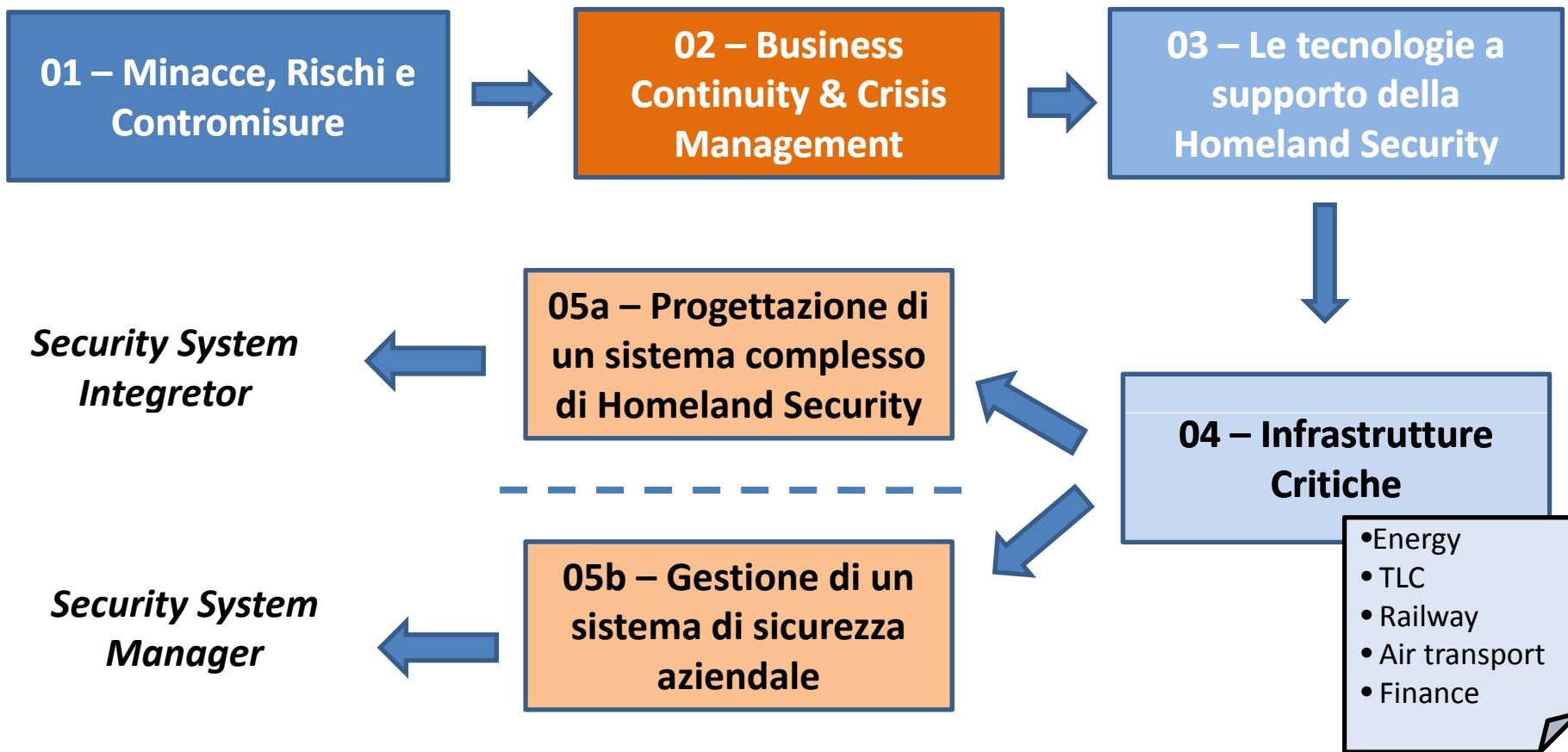
- Prof. Roberto Setola (Univ. Campus Bio-Medico di Roma & AIIC)
- Prof.ssa Marcella Trombetta (Univ. Campus Bio-Medico , Vice Direttore)

Comitato Scientifico

- Ing. Luigi D'Angelo (Protezione Civile)
- Dott. Dario De Marchi (Responsabile Ufficio Stampa Ministero dello Sviluppo Economico)
- Dott. Francesco di Maio (Responsabile Security ENAV)
- Ing. Alfonso Farina (Selex Sistemi Integrati)
- Dott. Franco Fiumara (Responsabile Protezione Aziendale FS)
- Prof. Giorgio Franceschetti (Università Napoli Federico II)
- Prof. Luigi Glielmo (Università Sannio)
- Dott. Giuseppe Lasco (Direttore Sicurezza Aziendale Terna)
- Dott. Francesco Lambiase (BCManager)
- Prof. Stefano Panzieri (Università Roma Tre)
- Ing. Concetta Pragliola (Ansaldo STS)
- Dott. Giorgio Riondino (Capo di Gabinetto Ministro per l'Attuazione del Programma di Governo)
- Dott. Damiano Toselli (Responsabile Security Telecom Italia)
- Dott. Umberto Saccone (Responsabile Security ENI)
- Prof. Giuseppe Sciutto (Presidente NITEL)
- Dott. Giuseppe Vozza (Responsabile Sicurezza Gruppo ENEL)
- Dott. Domenico Vulpiani (Dirigente Generale della Polizia di Stato Consigliere per la Sicurezza Informatica e per la protezione delle Infrastrutture Critiche del Ministero dell'Interno)



Master in Homeland Security - il programma



Testimonianze dei protagonisti, case study, visite a centri di eccellenza

Master in Homeland Security – i moduli

01 – Minacce, Rischi e Contromisure

Elementi normativi, gestionali, ed organizzativi. Metodologia e strumenti per l'analisi del rischio e delle vulnerabilità

Si intendono fornire gli strumenti di base per lo sviluppo di un sistema di sicurezza basato sull'analisi, classificazione e valutazione del rischio, della sua modellazione e gestione attraverso un rigoroso processo che parte dalla analisi delle minacce, delle vulnerabilità e di scenario fino all'individuazione dei possibili impatti e contromisure. Verranno forniti elementi di storia e geopolitica internazionale, fondamenti di diritto, fondamenti di economia, aspetti assicurativi e di trasferimento del rischio, nonché nozioni di normativa tecnica, circa gli standard per quel che riguarda il management di componenti e di sistemi di sicurezza.

02 – Business Continuity & Crisis Management

Prevenzione e gestione degli incidenti e delle situazioni di crisi.
Sistemi e procedure di Business Continuity e Disaster Recovery.
La comunicazione in situazioni di emergenza.

Il modulo ha l'obiettivo di fornire quegli strumenti metodologici ed operativi utili per comprendere i problemi connessi con la gestione delle emergenze, nelle tre dimensioni di prevention, incident handling e crisis management inclusi gli aspetti connessi con la comunicazione verso i media e i cittadini durante una crisi.

03 – Le Tecnologie a Supporto della Homeland Security

Illustrazione delle principali tecnologie impiegate nell'ambito della Homeland Security

I processi di controllo del territorio e di mantenimento della sicurezza si avvalgono di strumenti tecnologici di varia natura che consentono da un lato di accrescere la capacità di prevenire le azioni criminose (o gli eventi accidentali capaci di compromettere la sicurezza del servizio e/o dell'infrastruttura) e dall'altro di rilevare nel loro incipit, caratterizzare meglio situazioni di crisi e di affrontarle con maggiore efficacia. Questo modulo ha l'obiettivo di illustrare le principali tecnologie oggi utilizzate evidenziandone potenzialità e limiti e sulle prevedibili evoluzioni future

04 – Infrastrutture Critiche

Modellistica ed analisi delle principali infrastrutture: energetiche, di trasporto, di telecomunicazione e finanziarie

Questo modulo fornisce gli elementi teorici fondamentali per comprendere le modalità di funzionamento, le architetture e le tecnologie che caratterizzano le principali infrastrutture (trasporto ferroviario, aereo, stradale, di comunicazione, energetiche e finanziarie). Tali elementi sono essenziali per caratterizzare le principali vulnerabilità e minacce che possono affliggere tali strutture e sono un prerequisito essenziale per la progettazione di un efficace sistema di security e di Business Continuity/Crisis Management in grado di tener conto delle problematiche indotte dai sempre più estesi fenomeni di interdipendenza.

Percorso Security System Integrator

Mira a formare professionisti in grado di progettare, sulla base delle necessità di sicurezza, delle peculiarità del contesto e dello stato dell'arte della tecnologia, sistemi di sicurezza che siano le adeguate soluzioni tecnologiche/operative alle specifiche problematiche di sicurezza

Al termine del percorso lo studente sarà in grado di concepire e progettare un sistema di sicurezza integrato capace di contrastare le varie minacce in modo efficace, conforme alle normative e in linea con i risultati attesi dell'analisi dei rischi

Master in Homeland Security – i percorsi

Percorso Security System Manager

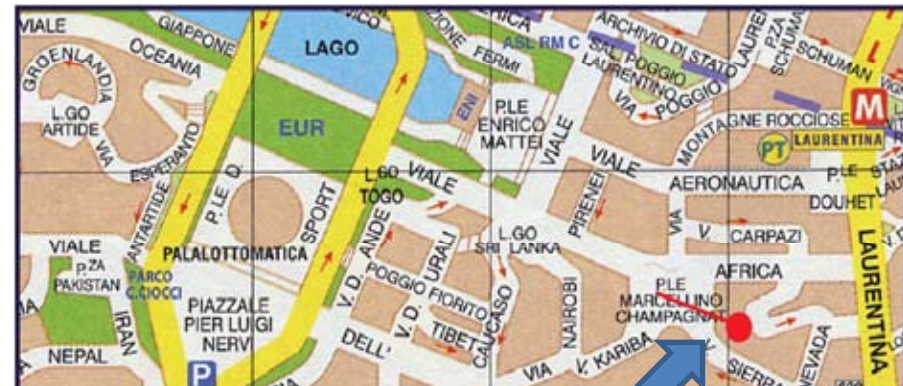
Mira a formare professionisti che, sulla base di una conoscenza del dominio applicativo, delle realtà territoriali e delle tecnologie esistenti, siano in grado di definire i necessari requisiti per i sistemi di sicurezza, di elaborarne gli obiettivi in termini di specifiche funzionali, finanziarie e contrattuali, di valutarne dinamicamente l'efficienza e l'efficacia e di gestirne l'utilizzo sia in condizioni di operatività normale sia in presenza di eventi anomali/crisi.

Al termine del percorso lo studente sarà in grado di analizzare, definire e gestire complessi sistemi di sicurezza e di crisis management inclusi gli aspetti connessi con la comunicazione verso i media e i cittadini

Master in Homeland Security - date

- Termine iscrizione: **26 Novembre 2010**
- Selezione candidati: 3 Dicembre 2010
- Inizio lezioni: 16 Dicembre 2009
- Termine Master: Dicembre 2011

Le lezioni si svolgeranno per l'intera giornata del giovedì e del venerdì di norma a settimane ed una volta al mese il sabato mattina

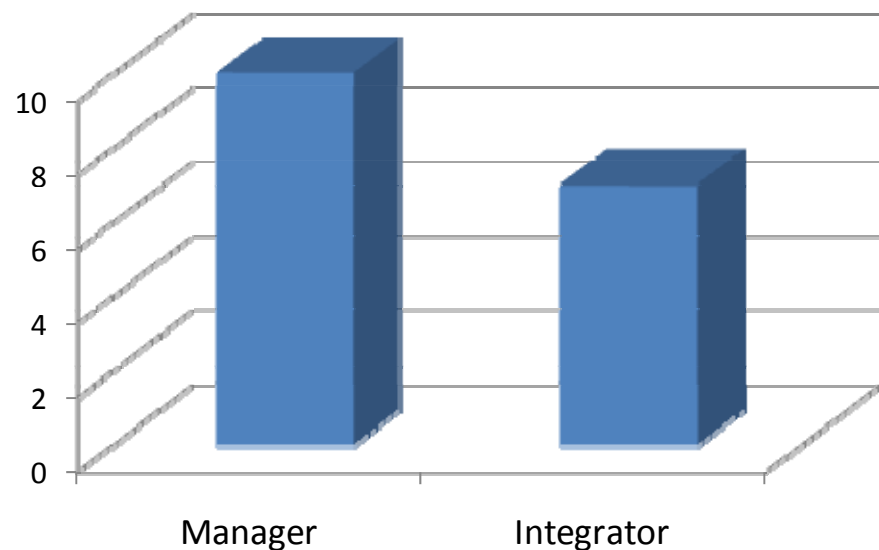


Aula Magna della RUI, viale Africa 27
(zona Metro B – Laurentina)

Risultati II ed. (a.a. 2009-10)

18 iscritti

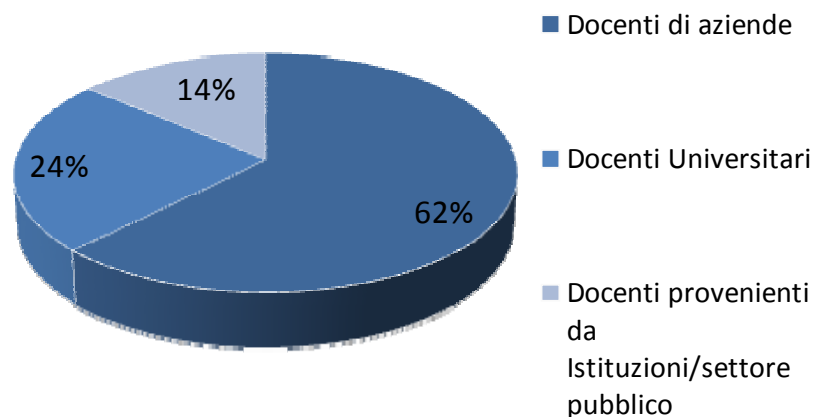
- di cui provenienti da **aziende partner** del master: 8
- provenienti da altre aziende: 4
- impiegati **PA**/organizz.internazionali: 2
- **neolaureati**: 4



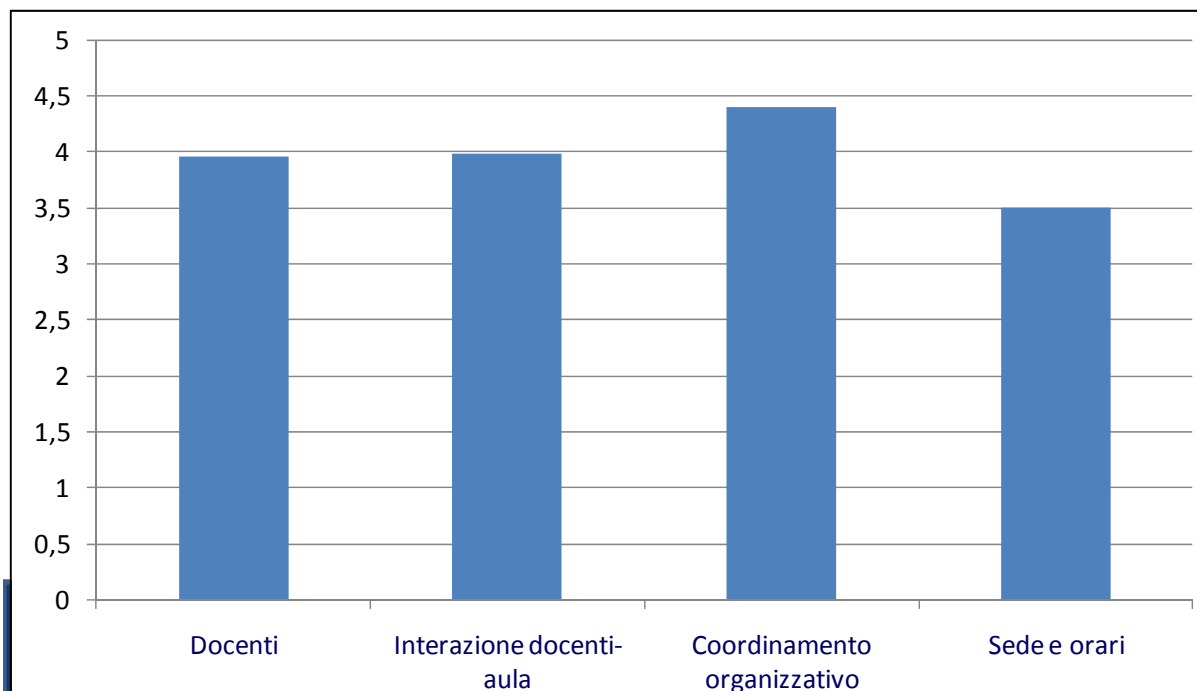
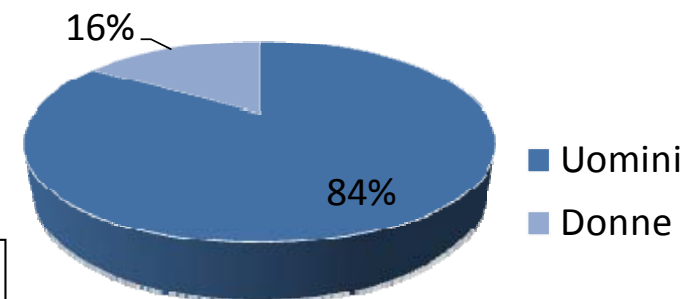
- numero di ore di **lezioni** frontali: 316
- numero **moduli** didattici: 5
- numero **esercitazioni** pratiche/simulazioni: 5
- numero **esami in itinere**: 3
- media voti riportati: 26,5/30
- numero **visite** guidate: 3

Risultati II ed. (a.a. 2009-10) - Docenti

Provenienza



La Faculty ha compreso **100** docenti, tra cui i responsabili della sicurezza delle principali realtà industriali ed istituzionali italiane e professori universitari esperti di Homeland Security



Ottima valutazione da parte dei discenti sia per quel che riguarda la Faculty, gli argomenti e l'organizzazione del Master

Cybersecurity

Fra i soggetti che hanno svolto una audizione davanti al COPASIR nell'ambito delle attività su **“sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico”**, compaiono **3** docenti del Master (Vulpiani, Toselli e Chiesa)

Camera dei Deputati — 14 —

XVI LEGISLATURA — DISEGNI DI LEGGE E RELAZIONI

minacce per la sicurezza nazionale derivanti dallo spazio cibernetico. È stato altresì stabilito di acquisire pareri di esperti per supportare utilmente il Comitato nella completa Relazione al Parlamento sul tema.

Sono stati quindi affidati incarichi di consulenza al dottor **Domenico VULPIANI**, per inquadrare il tema strategico, tecnologico e normativo; al dottor **Damiano TOSELLI**, presidente del Centro studi internazionale (CESI) per analizzare i rischi per la sicurezza nazionale in ambiti governativi e militari, e al dottor **Raoul CHIESA**, OSINT, per l'analisi delle eventuali ricadute del cybercrime sui civili ed economici, tra cui energia e servizi finanziari e trasporti. Ha partecipato, inoltre, alla audizione del dottor Gianluca Ansalone.

Il Comitato ha svolto le audizioni:

- il 2 dicembre 2009 del colonnello Umberto Ansalone, direttore del Nucleo speciale frodi telematiche della Guardia di finanza;

- il 16 marzo 2010 del Prefetto Giovanni De Santis, Direttore generale del DIS;

- il 14 aprile 2010 del dottor **Domenico VULPIANI**, Consigliere per la sicurezza informatica e la protezione delle infrastrutture critiche della Polizia di Stato;

- il 28 aprile 2010 dei rappresentanti delle società Telecom Italia (dottor **Damiano TOSELLI**), Vodafone (dottor Gaetano COSCIA), Wind (dottor Vincenzo FOLINO) e H3G (dottor Roberto COSA);

- il 18 maggio 2010 del dottor **Raoul CHIESA**, consulente del FUNICRI;

- il 20 maggio 2010 dell'ambasciatore Giancarlo ARAGONA, nella sua qualità di membro del Gruppo di Riflessione Strategica della NATO, impegnato nella definizione del nuovo concetto strategico dell'Alleanza;

- il 1° luglio 2010 di un alto rappresentante del sistema di sicurezza di un governo europeo, con l'obiettivo di valutare le politiche di contrasto alla minaccia adottate in quel Paese.

Inoltre, in data 6 maggio 2010, il presidente del Comitato, onorevole Massimo D'Alema, d'intesa con il relatore, senatore Francesco Rutelli, ha inviato a soggetti istituzionali e società, individuati per la loro particolare e specifica competenza nel settore, una richiesta volta a conoscere le loro valutazioni « sull'evoluzione della minaccia e le tendenze prevedibili; sulle strategie di prevenzione adottate sotto il profilo aziendale, sul contributo alla tutela delle infrastrutture critiche nazionali, nonché sulla qualità della collaborazione con le istituzioni preposte ».

CAMERA DEI DEPUTATI

SENATO DELLA REPUBBLICA

XVI LEGISLATURA

Doc. XXXIV
n. 4

COMITATO PARLAMENTARE PER LA SICUREZZA DELLA REPUBBLICA

(istituito con la legge 3 agosto 2007, n. 124)

(composto dai deputati: D'Alema, Presidente; Pastore, segretario, Briguglio, Cicchitto e Rosato e dai senatori: Esposito, Vicepresidente; Caforio, Passoni, Quagliariello e Rutelli)

RELAZIONE

sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico

(Relatore: sen. Francesco RUTELLI)

Approvata nella seduta del 7 luglio 2010

Trasmessa alle Presidenze delle Camere il 15 luglio 2010

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

Master in Homeland Security - informazioni

www.masterhomelandsecurity.eu/



Università Campus Bio-Medico
Scuola di Formazione Continua
Via Álvaro Del Portillo, 21
00128 Roma
Tel.: 06.22.541.9300
Fax: 06.22.541.1900
E-mail: sfc@unicampus.it

Dott. Maurizio Virone
m.virone@unicampus.it
Tel.: 06.22541.9305

Dott.ssa Rossella Liaci
rossella@nitel.it
Tel.: 06. 85344 238