



ISPAC
*International Scientific and Professional
Advisory Council
of the United Nations
Crime Prevention and Criminal
Justice Programme*



Conferenza internazionale su
CYBERCRIME: Globalità del fenomeno e sfide

promossa da
International Scientific and Professional Advisory Council of the United Nations
Crime Prevention and Criminal Justice Programme-ISPAC
Centro Nazionale di Prevenzione e Difesa Sociale-CNPDS
Fondazione Courmayeur

in cooperazione con
United Nations Office on Drugs and Crime-UNODC, Vienna
Korean Institute of Criminology - KIC, Seoul

Courmayeur Mont Blanc, Italy, 2-4 dicembre 2011
Hôtel Pavillon

FONDAZIONE CRT

Lo sviluppo delle nuove tecnologie dell'informazione e della comunicazione, *Information and Communication Technologies* (ICT), comprendenti l'uso di computer e database, ha modificato radicalmente il funzionamento della nostra società. Le agenzie governative e le imprese sono supportate da reti informatiche e conservano le informazioni su supporti elettronici. Le persone usano Internet per ogni genere di attività, dall'*e-commerce* all'*e-banking*, o mantengono contatti attraverso i *social network*. Nello stesso tempo, questa proliferazione delle tecnologie informatiche e della comunicazione ha causato un incremento di varie forme di reati informatici, che costituiscono una minaccia non solo per la riservatezza, l'integrità o la disponibilità dei sistemi informatici, ma anche per la sicurezza delle infrastrutture di importanza critica. I sistemi informatici, Internet, i *database*, ecc. sono diventati degli strumenti criminali, cioè un'opportunità per facilitare l'esecuzione di reati tradizionali come la frode o l'estorsione, ed un veicolo per nuovi tipi di reati, che emergono parallelamente alle nuove tecnologie. Il *cybercrime*, ovvero l'uso illecito delle tecnologie informatiche e della comunicazione è, infatti, comparso nella nostra vita quotidiana sotto diverse forme. I crimini informatici, inoltre, non sono limitati dai confini nazionali, sfruttano spesso le carenze disciplinari del sistema della giustizia penale (forze dell'ordine, procedimenti penali, magistratura, ecc.), per essere attuati e prosperare in un contesto di impunità virtuale.

Negli ultimi anni, la comunità internazionale ha capito la necessità di conoscere più a fondo questo nuovo crimine transnazionale e di iniziare a combatterlo. Questo è quanto espresso nei mandati sempre più importanti che le Nazioni Unite, compreso l'UNODC, United Nations Office on Drugs and Crime (Ufficio delle Nazioni Unite contro la Droga e il Crimine) hanno ricevuto dagli Stati Membri e dagli enti governativi.

L'11° Congresso delle Nazioni Unite su Prevenzione del Crimine e Giustizia Penale, tenutosi a Bangkok, in Thailandia nel 2005, aveva riconosciuto la gravità del *cybercrime*, anche con l'organizzazione di un workshop sui crimini informatici. La Dichiarazione di Bangkok sulle Sinergie e sulle Risposte: Alleanze Strategiche nella Prevenzione del Crimine e nella Giustizia Penale, approvata dalla risoluzione 60/177 dell'Assemblea Generale del dicembre 2005, ha appoggiato gli sforzi mirati al rafforzamento ed all'intensificazione della cooperazione esistente per prevenire, investigare e perseguire penalmente i reati collegati all'informatica ed all'alta tecnologia.

Nel 2010, il 12° Congresso delle Nazioni Unite su Prevenzione del Crimine e Giustizia Penale, tenutosi a Salvador de Bahia, in Brasile, incentrato in particolare sui crimini informatici, ha ottenuto due risultati molto concreti. La Dichiarazione di Salvador ha raccomandato all'UNODC di fornire assistenza tecnica e attività formativa agli Stati che lo richiedano,

per migliorare le legislazioni nazionali e permettere alle autorità nazionali di combattere i reati informatici. Inoltre, nella Salvador Declaration vi è una raccomandazione ad UNODC di convocare un gruppo intergovernativo di esperti per effettuare uno studio approfondito sul problema dei reati informatici e delle iniziative intraprese dagli Stati Membri, dalla comunità internazionale e dal settore privato. Il primo incontro di questo gruppo aperto di esperti intergovernativo ha avuto luogo dal 17 al 21 gennaio 2011: il gruppo ha, tra l'altro, validato gli argomenti, la metodologia e le tempistiche dello studio. Entrambi i mandati sono stati successivamente reiterati dalla Commissione sulla Prevenzione del Crimine e sulla Giustizia Penale (Commissione sul Crimine), dal Consiglio Economico e Sociale e dall'Assemblea Generale nella risoluzione 65/230.

Nell'aprile 2011, la Commissione sul Crimine ha adottato due risoluzioni aventi per oggetto il lavoro svolto dall'UNODC sul *cybercrime*, sottolineando l'importanza dei mandati della Dichiarazione di Salvador: la risoluzione 20/7 sulla promozione delle attività per combattere i reati informatici, comprendenti assistenza tecnica e attività di *capacity-building*, che ha richiesto ad UNODC di continuare a fornire, su richiesta, assistenza tecnica e attività formativa agli Stati, sulla base delle esigenze nazionali, in particolare per quanto riguarda la prevenzione, l'individuazione, l'investigazione ed il perseguire penalmente tutte le forme di reati informatici; e la bozza di risoluzione I (attualmente in corso di approvazione all'ECOSOC) su "Prevenzione, tutela e cooperazione internazionale per combattere l'uso delle nuove tecnologie dell'informazione nell'abuso e nello sfruttamento dei minori".

È chiaro che, pur essendo state intraprese molte iniziative, esiste ancora la necessità di migliorare l'attività di *capacity-building*, l'assistenza tecnica, la reciproca assistenza legale e la cooperazione internazionale per combattere i crimini informatici. Prevenire in modo efficace e perseguire penalmente i reati informatici richiede, innanzitutto, la conoscenza del problema da parte del pubblico in generale e indagini penali coordinate. Devono essere forniti assistenza tecnica e strumenti formativi per incrementare la capacità di combattere questi reati da parte dei paesi in via di sviluppo. Ciò permetterà loro, non solo di condividere conoscenze e informazioni per poter identificare, investigare e perseguire i crimini informatici in modo adeguato, ma anche per colmare il cosiddetto *digital divide*, cioè il divario digitale, in questo campo, tra i paesi in via di sviluppo e i paesi sviluppati.

In realtà, la preoccupazione è che, considerato il quadro giuridico contraddittorio e disomogeneo e la mancanza di capacità, molti paesi siano delle potenziali zone grigie dai quali i criminali informatici potrebbero operare per commettere impunemente i loro crimini nel resto del mondo. Queste tendenze di ricerca di "porti sicuri" possono già essere osservate e

dimostrate. È, quindi, essenziale migliorare le capacità nei paesi che risultano essere i meno sviluppati in tal senso.

Combattere il *cybercrime* è particolarmente difficile a causa dei problemi di giurisdizione che sorgono a livello nazionale e internazionale. Le forme tradizionali di giurisdizione si basano sul concetto di confini, e le leggi si basano sulla "sovranità territoriale". Poiché il cyberspazio non ha confini fisici, i criminali, nel mondo informatico, possono cambiare le loro sedi da un paese all'altro in pochi secondi, indipendentemente da dove si trovano fisicamente. Di conseguenza, tutti gli Stati devono essere in grado di usare e contribuire alla creazione di meccanismi di cooperazione internazionale. Ciò si rivela particolarmente importante nel caso dei paesi in via di sviluppo in quanto spesso sono tecnologicamente meno in grado di combattere i reati informatici e, quindi, particolarmente vulnerabili ad essere usati come piattaforme da cui organizzarli.

Alla luce di quanto precede, è fondamentale che gli Istituti della rete PNI delle Nazioni Unite abbiano l'opportunità di discutere, durante la Conferenza ISPAC 2011, della sfida globale rappresentata dal *cybercrime* e delle contromisure adottate e da adottare per combatterlo. La Sessione I della Conferenza sarà dedicata alla ricerca dell'equilibrio corretto tra sicurezza e libertà civili nella lotta contro i crimini informatici, attraverso il dibattito su argomenti che rientrano nell'ambito dei Diritti Umani nell'Era Tecnologica. Privacy, libertà di espressione ed altri diritti fondamentali saranno esaminati da esperti, accademici e altre istituzioni attirando l'attenzione di numerosi paesi del mondo. La Sessione II esaminerà, in particolare, lo sviluppo tecnologico ed gli speakers tratteranno casi specifici, quali reati sui dati, reati nella rete, reati di accesso ed altri. Nella Sessione III i relatori esamineranno la lotta contro il *cybercrime* da parte delle Forze dell'Ordine e delle Forze Investigative a livello dei paesi. L'assenza di politiche e procedure formali, come pure le difficoltà nel condividere le informazioni si riveleranno gli ostacoli principali alla cooperazione internazionale. Gli istituti di ricerca del PNI avranno l'obiettivo di esigere degli sforzi di maggiore cooperazione a livello nazionale ed internazionale per adempiere al meglio ai propri compiti.

PROGRAMMA

Venerdì 2 dicembre
ore 15.00

Seduta di Apertura

- LODOVICO PASSERIN d'ENTRÈVES, *Fondazione Courmayeur*
- FABRIZIA DERRIARD, *sindaco di Courmayeur*
- LIVIA POMODORO, *presidente, Tribunale di Milano; presidente CNPDS/ISPAC*
- KIM IL-SU, *President, Korean Institute of Criminology - KIC*

ore 15.30

Allocuzione Introduttiva

JOHN SANDAGE, *Director Division for Treaty Affairs, and Chief, Organized Crime and Illicit Trafficking Branch, United Nations Office on Drugs and Crime -UNODC*

ore 16.00

SESSIONE I

SICUREZZA E LIBERTÀ CIVILI NELLA LOTTA CONTRO IL *CYBERCRIME*

Presiede e introduce

ULRICH SIEBER, *Director and Head, Criminal Law Section, Max-Planck Institute*

- Libertà e sicurezza un giusto equilibrio nel contrasto al Cybercrime: sfide per la Network Society
EMILIO VIANO, *Professor, Department of Justice, Law and Society, American University & Washington College of Law, Washington DC*

ore 17.00

Coffee Break

- Principi giuridici fondamentali per una proposta ponderata
GIOVANNI BUTTARELLI, *Assistant European Data Protection Supervisor, EDPS, Brussels*
- BEN HAYES, *Statewatch - Monitoring the State and Civil Liberties in Europe, London, UK*

ore 18.30

Dibattito

Sabato 3 dicembre
ore 9.00

SESSIONE II

CASE STUDIES NEL CYBERCRIME

Presiede

JOON OH JANG, *Senior Research Fellow, Director of International Center for Criminal Justice, Korean Institute of Criminology (KIC)*

- **Uniti contro il *cybercrime*: L'iniziativa di *capacity-building* di UNODC/ITU per combattere la criminalità informatica**
GILLIAN MURRAY, *Chief, Focal Point for Cybercrime, Conference Support Section, Division for Treaty Affairs UNODC*
CARLA LICCIARDELLO, *Project Officer on Cybersecurity, International Telecommunication Union (ITU)*
- **Esplorando nel mercato internazionale a proposito della sottrazione dei dati e degli attacchi informatici**
THOMAS HOLT, *Associate Professor, School of Criminal Justice Michigan State University, USA*
- **Modalità di scelta delle vittime dei reati informatici**
K. JAISHANKAR, *Department of Criminology and Criminal Justice, Manonmaniam Sundaranar University, Executive Director, Centre for Cyber Victim Counselling, India*

ore 11.00

Coffee Break

ore 11.30

SESSION II Continua

Presiede

DUNCAN CHAPPELL, *Professor of Criminal Law, Faculty of Law, University of Sydney*

- **ROB McCUSKER, *Director of Centre for Fraud and Financial Crime, University of Teesside Middlesbrough, UK***
- **Il punto di vista di Europol sul Cybercrime**
ROBERTO FERNANDEZ ALONSO *Europol Cybercrime Center, The Netherlands*

Dibattito

ore 13.00

Lunch

ore 15.00

SESSIONE III

FORZE DELL'ORDINE E FORZE INVESTIGATIVE NAZIONALI IN CAMPO CONTRO IL *CYBERCRIME*

Presiede

LUIS ARROYO ZAPATERO, *Director; Instituto de de Derecho Penal Europeo e Internacional, Ciudad Real, España*

- La nuova legge penale cinese in materia di Cybercrime nella rete globale
PI YONG, *Professor School of Law, Wuhan University, China*
- WONSANG LEE, *Associate Research Fellow, Korean Institute of Criminology, South Korea*
- Cyber Criminal Law; prospettive politiche e legislazione in Iran
BATOUL PAKZAD, *Associate Professor, Ph.D of Criminal Law and Criminology, Legal Consultant, Ministry of Justice, I.R. of Iran*
GHASSEM GHASSEMI, *Lawyer and Lecturer at Law, Islamic Azad University, Teheran, I.R. of Iran*

ore 17.30

Dibattito

Domenica 4 dicembre
ore 9.00

SESSIONE IV

NUOVE RISPOSTE GIURIDICHE NAZIONALI ED INTERNAZIONALI AL *CYBERCRIME*

Presiede

GILLIAN MURRAY, *Chief, Focal Point for Cybercrime, Conference Support Section, Division for Treaty Affairs UNODC*

- 10 anni dopo la Convenzione di Budapest: quali insegnamenti?
ALEXANDER SEGER, *Secretary Cybercrime Convention Committee and Head of Data Protection and Cybercrime Division, Council of Europe, Strasburg*
- Potenziali nuovi strumenti giuridici globali nel

contrasto al Cybercrime

STEIN SCHJOLBERG, *Judge, Co-chair of the EastWest Institute (EWI) Cybercrime Legal Working Group, Oslo*

- Attuali tendenze di armonizzazione nella legislazione sul Cybercrime

MARCO GERCKE, *Director, Cybercrime Research Institute, Köln University, Germany*

- Autodifesa dal Cybercrime

MIGUEL ONTIVEROS ALONSO, *Director of the National Institute for Criminal Science of Mexico, Mexico (OAS)*

Dibattito

Conclusioni e Raccomandazioni

STEFANO MANACORDA, *professore di diritto penale, Università di Napoli II, Italia; Università di Parigi I, Francia; vice presidente ISPAC Board*

ore 11.00

ore 11.30

Sede dei lavori
Sala Conferenze, Hôtel Pavillon
Via Regionale, 62 - 11013 Courmayeur (AO)

Lingue ufficiali
inglese e italiano con traduzione simultanea

Segreteria della Conferenza
Fondazione Centro nazionale di prevenzione e difesa sociale-CNPDS
Palazzo Comunale delle Scienze Sociali
3, Piazza Castello - 20121 Milano MI
Phone: +39 02 86.46.07.14 - Fax: +39 02 72.00.84.31
E-mail: cnps.ispac@cnps.it - Home page: www.cnps.it
Home page: <http://ispac.cnps.org>