



EUROPE

THE ARTS
CHILD POLICY
CIVIL JUSTICE
EDUCATION
ENERGY AND ENVIRONMENT
HEALTH AND HEALTH CARE
INTERNATIONAL AFFAIRS
NATIONAL SECURITY
POPULATION AND AGING
PUBLIC SAFETY
SCIENCE AND TECHNOLOGY
SUBSTANCE ABUSE
TERRORISM AND
HOMELAND SECURITY
TRANSPORTATION AND
INFRASTRUCTURE
WORKFORCE AND WORKPLACE

This PDF document was made available from www.rand.org as a public service of the RAND Corporation.

[Jump down to document](#) ▼

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world.

Support RAND

[Browse Books & Publications](#)

[Make a charitable contribution](#)

For More Information

Visit RAND at www.rand.org

Explore [RAND Europe](#)

View [document details](#)

Limited Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law as indicated in a notice appearing later in this work. This electronic representation of RAND intellectual property is provided for non-commercial use only. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use.

This product is part of the RAND Corporation technical report series. Reports may include research findings on a specific topic that is limited in scope; present discussions of the methodology employed in research; provide literature reviews, survey instruments, modeling exercises, guidelines for practitioners and research professionals, and supporting documentation; or deliver preliminary findings. All RAND reports undergo rigorous peer review to ensure that they meet high standards for research quality and objectivity.

TECHNICAL
REPORT

Handbook of Legal Procedures of Computer and Network Misuse in EU Countries

Lorenzo Valeri, Geert Somers, Neil Robinson,
Hans Graux, Jos Dumortier

Prepared for the European Commission

The research described in this report was prepared for the European Commission.

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

RAND® is a registered trademark.

© Copyright 2006 the European Commission

All rights reserved. No part of this book may be reproduced in any form by any electronic or mechanical means (including photocopying, recording, or information storage and retrieval) without permission in writing from the copyright holder.

Published 2006 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
201 North Craig Street, Suite 202, Pittsburgh, PA 15213-1516
Newtonweg 1, 2333 CP Leiden, The Netherlands
Westbrook Centre, Milton Road, Cambridge CB4 1YG, United Kingdom
Uhlandstraße 14, 10623 Berlin, Germany
RAND URL: <http://www.rand.org/>
RAND Europe URL: <http://www.rand.org/randeurope>
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Executive Summary

This document represents one of the two main deliverables of the 2005 project to update the 2003 CSIRT Legal Handbook. It sets out in a concise form the legal status of different types of computer misuse under the legal systems of the EU countries. The study reviewed the information in the 2003 CSIRT Legal Handbook, which covered the 16 member states, and also included information relating to the new member states which joined in 2004. Information relating to the legal environment for dealing with cyber-crime in each member state was also accompanied by an indication of the prosecution policy of law enforcement agencies in the countries, along with standard rules or procedures for the collection, handling documentation and reporting of computer based evidence. Penal and civil law was considered where applicable.

The Country Reports section begins with an introduction to the supra-national legislative environment pertinent to cyber-crime. The chapters for each country are then presented alphabetically. They are kept concise to ensure brevity and usefulness for the user community. Each country chapter is split into the following sub-sections:

Legislation on Computer Crime

This sub-section presents a general overview of the extent and nature of computer crime legislation in the country. It details whether specific laws have been created to deal with computer crimes or whether these are covered under amendments to existing legislation (e.g. theft). It also highlights the existence of particular legislation to deal with spam or identity theft. This section also contains a table that indicates which penalty, under which law is applicable for a certain type of incident. The severity of the penalty is shown, as is the law under which it is prosecutable (known as applicable provision) and the legal description of the incident.

This sub-section also includes a table of incident types, along with the applicable legal provisions and the sanctions imposed in these provisions specifying the duration of imprisonment and the amount of the fines whenever possible. In order to obtain comparable results for all Member States, these incident types are fixed according to the taxonomy outlined earlier. In the rare event that no provisions apply to an incident, a note is simply made that there is "no applicable provision". Note that legal provisions can be criminal or administrative in nature. Both categories are included in the same table.

Also note that one incident can be covered by more than one provision and that one provision can apply to many incidents. Finally, it is even possible that one provision contains two or more different crimes with different sanctions.

Law Enforcement bodies

This sub-section indicates briefly which law enforcement organisations are present in the country, their structure, roles and estimated effectiveness. It also details the judicial system and what courts are most likely to deal with computer crime incidents and how the process works for appeals to a court of higher authority.

Reporting

This sub-section details the existence of reporting mechanisms in the country, including national schemes and non-national or voluntary activities.

Forensics

This sub-section details forensic procedures in common use in the country (for example, network searching and data seizure).

References

Finally, each chapter lists the references to the legal provisions themselves, including an English translation of the titles.