

Chapter 12

The Present Cybercrime: Operational and Instructive Experiences

Antonio Apruzzese
Italian National Police, Italy

EXECUTIVE SUMMARY

The preponderant role played by the computer means, which is the more and more direct aim of the criminal action through sophisticated computer technologies, incites to reconsider the classical criminological and victimological patterns. In fact, new kinds of criminality linked to the use of sophisticated computer technologies, which are taking up the state agencies in the activities of prevention and repression, have recently assumed aspects of great and worrying importance. So, the need to formulate suitable training course of the personnel of those police branch (Postal and Communication Police of the Italian National Police), specialized in countering the high tech crime, is becoming more and more compulsory.

BACKGROUND

The Italian National Police, since few years, has prepared and activated in the Police Communication Branch an agile and specific agency to counter those new threats of cyber criminality. To the creation of high specialized investigative units, which are wide-spread distributed on the whole Italian territory, this structure combines the activation of international links with analogous agencies that are operating in almost every country in the world. A constant

monitoring of the computer networks aims to the surveying and the prevention of any new kind of danger. The constitution, within the central service of the Postal and Communication Police, of the C.N.A.I.P.I.C. – National Anti-cybercrime Center for the protection of the critical infrastructure-, is particularly significant. The center is directed to the carrying out of efficacious forms to counter terrorist criminal computer attacks toward the so called critical infrastructures like, for instance, those of the energetic area, of the transport, of the communication and that of the e-government.

DOI: 10.4018/978-1-60566-872-7.ch012

INTRODUCTION

New kinds of criminality connected with the use of the high-tech information technology have recently assumed very important aspects.

The well known phenomenon of the “phishing”, the more and more frequent improper use of credit cards and other electronic means of payment have almost reached spreading and pervasiveness levels able to cause well-grounded worries in the whole economic and financial area, even because of the widespread fear of the rise of uncontrollable sensations of insecurity in the large number of the users.

The new criminal emergencies are seriously taking up the public agencies, which develop countermeasures and repression activities aiming, first of all, to the most complete global comprehension of the phenomenon, so to the definition of the most profitable investigative protocols.

In this context, the need to formulate suitable training courses of the human resources attached to the production departments becomes more important.

The topic is evidently stimulating the criminological scientific community too, very interested in new reformulations of the traditional concepts of offender typology, victimological profiles, the diversified aspects of the offender-victim of the crime relationship and the innovative kinds of criminal associative patterns which are now emerging.

The professional experience that we want to bear witness in the research came out, on the one hand, from a long term work in the police field (The Police Communication Branch of the Italian National Police) specialized in the fight against the high-tech crime, and, on the other hand from the training activities both of the personnel that is already employed in the operational units and the young people that are attending the Police Academies.

THE NEW CRIMINAL BUSINESS

The need to outline a general profile of the new kinds of cyber crimes issued from the concrete operational activity, which has been carried out in the field, cannot be postponed no longer.

Once it was the sole prerogative of subjects (for instance the well known hackers, crackers and others) with excellent computer and technical abilities who operated alone and autonomously and, very frequently, without any direct profit purpose. Nowadays, more and more frequently, those criminal events are closely linked with heterogeneous organizations that, having recourse to the most uncommon forms of recruitment of the essential technical experts, conduct the ranks of “corporations” that assure huge financial revenues pointing out new structural models in areas that are undoubtedly transnational.

NEW CYBERCRIMES

The new crimes, especially based on the digital identity theft, are mainly oriented to the sector of the online banking services, the monetics (automated monetary system composed by credit cards and electronic money in general) and the e-commerce.

The common and substantial characterizing element is the embezzlement of the confidential data, which permit the access and the availability of online bank accounts and the use of credit cards and other electronic means of payment.

In the e-commerce the digital identity theft is often used even to commit frauds in behalf of unaware third parties.

We clearly believe that transnational organized criminal groups are conducting the ranks of those innovative criminal activities insuring the highest profit and the lowest risk concerning the whole occidental world.

Among the most familiar online banking system attacks there is the so called “phishing”.

5 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/teaching-case/present-cybercrime-operational-instructive-experiences/37377

Related Content

A Rough Set Based Approach to Find Learners' Key Personality Attributes in an E-Learning Environment

Qinghua Qinghua Zheng, Xiyuan Wuand Haifei Li (2008). *International Journal of Web-Based Learning and Teaching Technologies* (pp. 29-56).

www.irma-international.org/article/rough-set-based-approach-find/3016

An Approach to Convert Conventional Laboratories Into IoT-Enabled Laboratories

Prakash K. R., Santhosh M. S., Purushothama G. K.and Ramya M. V. (2021). *International Journal of Web-Based Learning and Teaching Technologies* (pp. 108-120).

www.irma-international.org/article/an-approach-to-convert-conventional-laboratories-into-iot-enabled-laboratories/284473

Manual Label and Machine Learning in Clustering and Predicting Student Performance: A Practice Based on Web-Interactive Teaching Systems

Mengjiao Yin, Hengshan Cao, Zuhong Yuand Xianyu Pan (2024). *International Journal of Web-Based Learning and Teaching Technologies* (pp. 1-33).

www.irma-international.org/article/manual-label-and-machine-learning-in-clustering-and-predicting-student-performance/347661

Online Assessment in Programming Courses: A Multiple Case Study

Denise M. Woitand David V. Mason (2006). *Selected Styles in Web-Based Educational Research* (pp. 111-128).

www.irma-international.org/chapter/online-assessment-programming-courses/28774

Learning and Teaching Styles for Teaching Effectiveness: An Empirical Analysis

Anshu Saxena Arora, Reginald Leseaneand Mahesh S. Raisinghani (2011). *International Journal of Web-Based Learning and Teaching Technologies* (pp. 1-13).

www.irma-international.org/article/learning-teaching-styles-teaching-effectiveness/55552