Chapter 39
Towards a Cyber–Destructors Assessment Method

Francisco V. Cipolla-Ficarra
ALAIPO – AINCI, Spain and Italy

Alejandra Quiroga
Universidad Nacional de La Pampa, Argentina

Jacqueline Alma
Electronic Arts – Vancouver, Canada

ABSTRACT
This chapter shows the first results of a technique based on the information from Web 2.0 that can speedily and economically detect the networks or people who play, anonymously or not, the role of cyberdestructors. The group of presented examples is useful to probe the modus operandi of the cyberdestroyers of the online information systems and the democratic promotion of scientific knowledge in the future generations of users of interactive systems both online and offline. Finally, the chapter reveals the main patterns of behaviour of a cyberdefender in the context of social networks.

INTRODUCTION
The momentum of the Internet would bring in its wake a series of problems related not only to the safety of the digital information, but also the appearance of pressure groups who take advantage of the anonymity of the net to attack everything which does not play by their rules, credos or other formulas who attempt against the freedom of people and democracy in the digital information society. The origin of these destructive behavior can be related to a legend of the European middle ages when in 1412 three Spanish knights from Toledo belonging to a brotherhood or fraternity called Garduña (Garduña, 2012), reached a small island of the Mediterranean (Favignana) and after setting down a series of rules for their members they headed for the current territories of Calabria, Naples and Sicily setting in motion illegal and destructive organizations. From there they would extend to the whole of Europe and the rest of the world.

DOI: 10.4018/978-1-4666-4490-8.ch039
Towards a Cyber-Destructors Assessment Method

Actually, these rules are still in force for these brotherhoods. Obviously the Internet is another tool at the disposal of these or other international criminal brotherhoods or associations with limited costs and with an almost worldwide scope of their operations. The main goal is always the same: smearing people, attack institutions, breeding conflicts, etc. Now from the technological point of view there is a wide set of applications and mechanisms stemming from the software and the hardware to prevent unauthorized access to the personalized information with the purpose of tutoring the privacy of the information, such as: firewalls, antivirus, software applications or specialized electronic devices, for instance. Besides, the legislation to tutor the computer users or other devices to receive and send digital information, it is very varied, lax and sometimes ineffective. The inefficacy is mirrored in an aspect which is not currently taken into account in the legislation for these issues, that is, the speed in detecting, stopping and repairing the damages caused in the face of unfair and unworthy attacks stemming from those who directly or indirectly receive orders from the brotherhood of their belonging. In this sense we understand by “brotherhood of belonging or medieval” to those members who use the informatics media and the Internet to spread false information with destructive purposes. This factor in the current work will also be known under the notion of “medieval brotherhood”. One of the features that characterize that medieval brotherhood is that all its members behave in the same way because their acts are ruled following a set of norms or rules, which are established and maintained along the centuries and which not have changed with the new technologies. In the era of the expansion of communicability it is easy to observe how the behavior of the medieval brotherhood stays identical, in all the geography of our planet. These first conclusions are obtained thanks to the analysis of the contents and the communicability in the social networks.

In this sense we have already detected the behavior of the young members (Cipolla-Ficarra & Kratky, 2011) who devoted themselves to modifying the counter of visitors in a website which works with Linux, thanks to open source software applications stemming from Russia. Whereas the administrators of the system, webmaster, designers, etc. must follow a whole procedure to access the website (two passwords, timetable to which wants to have access, captcha (Completely Automated Public Turing test to tell Computers and Humans Apart) system to have access to the server where the website is to be found. The destructive behavior consisted in altering the numeration or directly eliminating it as if it was a reset. In this regard this behavior temporally disappeared when other attacks were in motion allegedly from servers located in Russia, for instance, insertion of an organization in the spam distributors list or in listings to continuously receive publicity from alleged servers located in Russia and which constantly change the sending addresses, leaving unusable the options to eliminate spam the users have at their disposal. These patterns of behavior which may seem trivial cause not only a loss of time but also international disrepute, as in the case of being inserted unfairly in the listings of those people who distribute spam. A priori they can be made by young computer users, who do not necessarily must have a great knowledge of computer science but rather contacts (Cipolla-Ficarra & Ficarra, 2012). An example is the case described in the Figure 2 and Figures 9 and 10 in the Appendix. That’s to say, from the social networks they may contact other people who know how to carry out these attacks, fostering the phenomenon of medieval brotherhood. Regrettably in