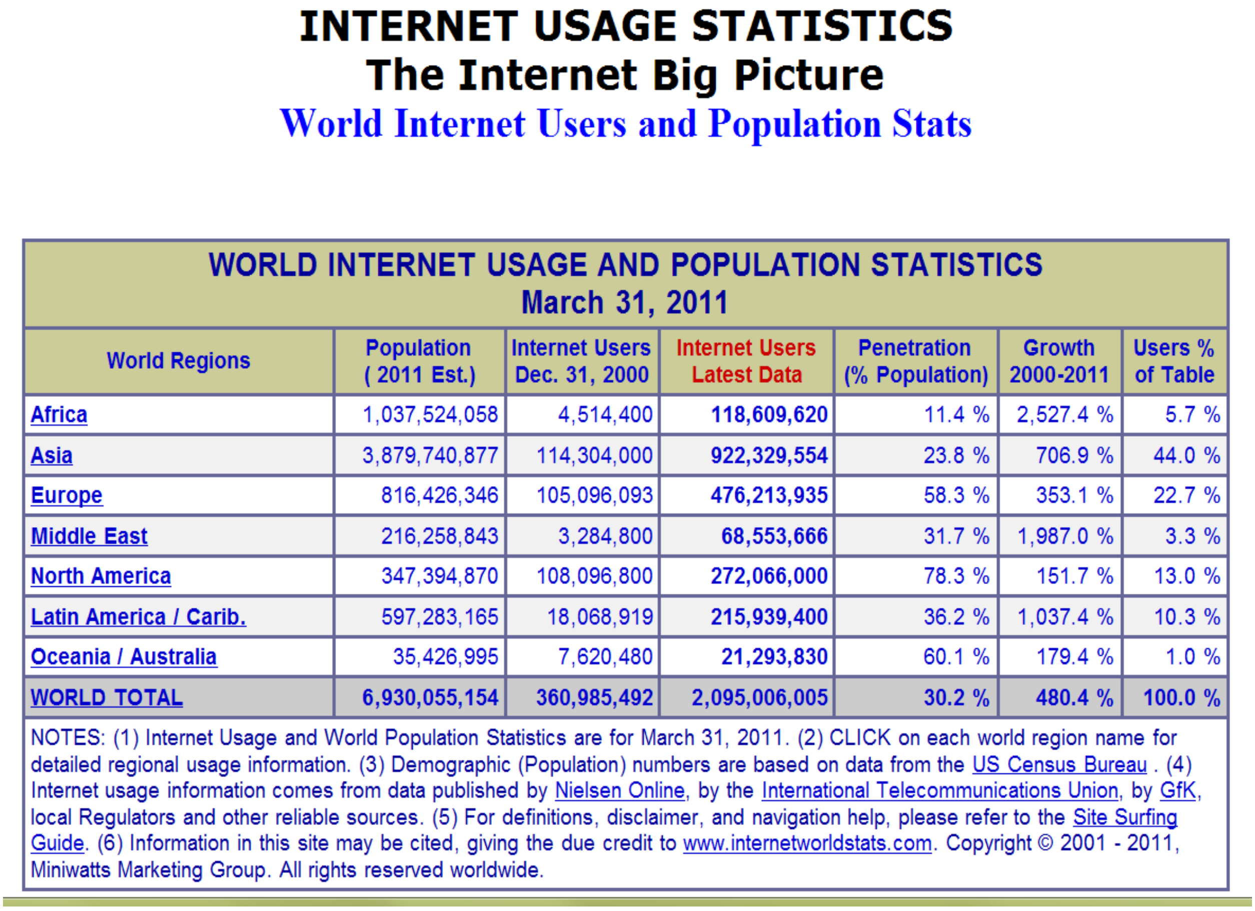
INTRODUCTION TO CYBERCRIME

Main Source:

Connolly, C. (2009) "Cyberlaw," *Hot Topics: Legal Issues In Plain Language,* No. 70, State Library of NSW. <http://www.legalanswers.sl.nsw.gov.au/hot_topics/pdf/cyberlaw_70.pdf>

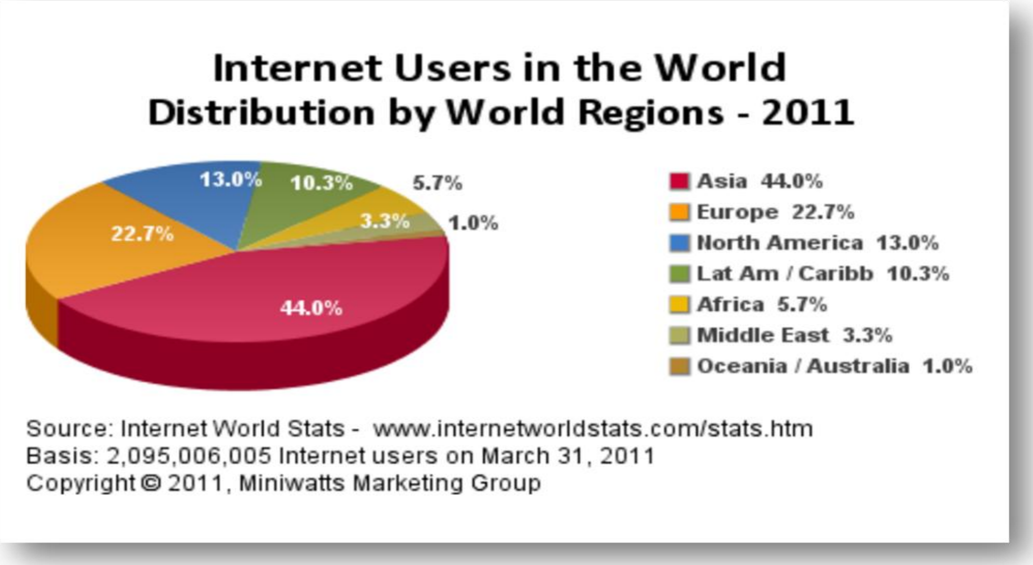


INTERNET USAGE STATISTICS
The Internet Big Picture
World Internet Users and Population Stats

WORLD INTERNET USAGE AND POPULATION STATISTICS
March 31, 2011

World Regions	Population (2011 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetration (% Population)	Growth 2000-2011	Users % of Table
Africa	1,037,524,058	4,514,400	**118,609,620**	11.4 %	2,527.4 %	5.7 %
Asia	3,879,740,877	114,304,000	**922,329,554**	23.8 %	706.9 %	44.0 %
Europe	816,426,346	105,096,093	**476,213,935**	58.3 %	353.1 %	22.7 %
Middle East	216,258,843	3,284,800	**68,553,666**	31.7 %	1,987.0 %	3.3 %
North America	347,394,870	108,096,800	**272,066,000**	78.3 %	151.7 %	13.0 %
Latin America / Carib.	597,283,165	18,068,919	**215,939,400**	36.2 %	1,037.4 %	10.3 %
Oceania / Australia	35,426,995	7,620,480	**21,293,830**	60.1 %	179.4 %	1.0 %
WORLD TOTAL	**6,930,055,154**	**360,985,492**	**2,095,006,005**	**30.2 %**	**480.4 %**	**100.0 %**

NOTES: (1) Internet Usage and World Population Statistics are for March 31, 2011. (2) CLICK on each world region name for detailed regional usage information. (3) Demographic (Population) numbers are based on data from the US Census Bureau . (4) Internet usage information comes from data published by Nielsen Online, by the International Telecommunications Union, by GfK, local Regulators and other reliable sources. (5) For definitions, disclaimer, and navigation help, please refer to the Site Surfing Guide. (6) Information in this site may be cited, giving the due credit to www.internetworldstats.com. Copyright © 2001 - 2011, Miniwatts Marketing Group. All rights reserved worldwide.



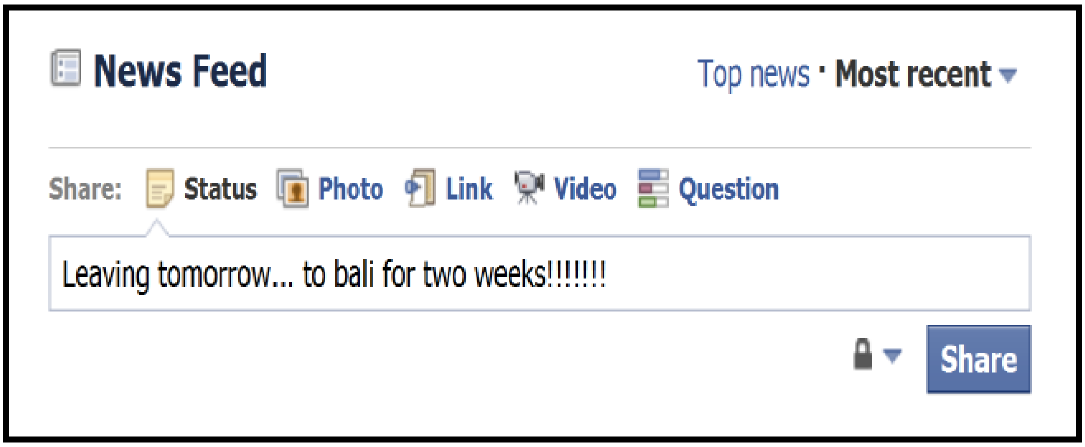
Source: Internet World Stats - www.internetworldstats.com/stats.htm
Basis: 2,095,006,005 Internet users on March 31, 2011
Copyright © 2011, Miniwatts Marketing Group

Types of Cybercrime

Types of Cybercrime	Description
Financial Crimes	Credit Card Frauds; Money Laundering
Cyber Pornography	Pornographic Websites; Online distribution
Online Gambling	Millions of websites, all hosted on servers abroad, offer online gambling.
IP Crimes	Software Piracy; Copyright Infringement; Trademarks Violations; Theft of Computer Source Code.
Email Spoofing	A spoofed email is one that appears to originate from one source but actually has been sent from another source.
Cyber Defamation	This occurs when defamation takes place with the help of computers and/or the Internet. E.g. someone publishes defamatory matter about another on a website.
Cyber Stalking	This involves following a person's movements across the Internet by posting messages (sometimes threatening) on bulletin boards frequented by the victim, entering chat-rooms frequented by the victim, constantly bombarding the victim with emails etc.
Unauthorised Access	Also known as Hacking. Involves gaining access illegally to a computer system or network and in some cases making unauthorized use of this access. Hacking is also the act by which other forms of cyber-crime (e.g., fraud, terrorism) are committed.
Theft	Theft of any information contained in electronic form such as that stored in computer hard disks, removal storage media, etc. Can extend to identity theft.
Email Bombing	This refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing.
Salami Attacks	These attacks are often used in committing financial crime and are based on the idea that an alteration, so insignificant, would go completely unnoticed in a single case. E.g. a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say 5 cents a month) from the account of every customer. This unauthorized debt is likely to go unnoticed by an account holder.
Denial of Service (DNS) Attack	This involves flooding a computer resource with more requests than it can handle, causing the resource (e.g. a web server) to crash thereby denying authorized users the service offered by the resource. Another variation to a typical denial of service attack is known as a Distributed Denial of Service (DDoS) attack wherein the perpetrators are many and are geographically widespread. It is very difficult to control such attacks and is often used in acts of civil disobedience.
Virus/worm	Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.
Logic Bombs	These are event dependent programs where programs kick into action only when a certain event (known as a trigger event) occurs. Some viruses may be termed logic bombs because they lie dormant throughout the year and become active only on a particular date (e.g. Chernobyl virus).
Trojan Attacks	An unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.
Web Jacking	This occurs when someone forcefully takes control of a website (by cracking the password and later changing it).
Cyber-Terrorism	Hacking designed to cause terror. Like conventional terrorism, `e-terrorism' is utilizes hacking to cause violence against persons or property, or at least cause enough harm to generate fear.

Cybercrime By Context

You and your “Friends”



Leaving tomorrow... to bali for two weeks!!!!!!

You and “the Cyber-Criminal”

- “US dismantles 'massive' cyber crime syndicate”, *BBC News,* 10 November 2011. <http://www.bbc.co.uk/news/business-15668377>

You and the (overly security-conscious) Government

- “Cybercrime bill has 'serious flaws'”, says Greens Senator Scott Ludlam”, *The Australian,* 18 August 2011. < http://www.theaustralian.com.au/australian-it/government/cybercrime-bill-has-serious-flaws-says-greens-senator-scott-ludlam/story-fn4htb9o-1226117589668>

You and “Cybercrime Inc.”

- “The Evolution of CyberCrime Inc.”, *New York Times,* 4 April 2008. <http://www.nytimes.com/2008/04/04/technology/04iht-cybercrime07.html?pagewanted=all>

- “Inside a global cybercrime ring”, *Boston, 24 March 2011.* <*http://www.reuters.com/article/2010/03/24/us-technology-scareware-idUSTRE62N29T20100324*>

Interesting Articles:

- “Facebook Makes Deal With German Privacy Group”, *New York Times,* 24 January 2011. <http://www.nytimes.com/2011/01/25/technology/25facebook.htm>

- “Google Fined For Street-view Privacy Breach”, *Huffington Post,* 21 March 2011. <http://www.huffingtonpost.com/2011/03/21/google-fined-for-street-v_n_838323.html>

Useful References

- Australian Crime Commission, “Crime Profile Series – Cybercrime”, April 2011. <http://www.crimecommission.gov.au/sites/default/files/files/cyber-crime.pdf>

Simple factsheet with a brief overview.

- Australian Computer Emergency Response Team, Australian High Tech Crime Centre, Australian Federal Police (AFP), New South Wales Police, Northern Territory Police, Queensland Police, South Australia Police, Tasmania Police, Victoria Police, Western Australia Police. (2006) “AusCERT Computer Crime and Security Survey,” *AusCERT*, University of Queensland. <http://www.auscert.org.au/images/ACCSS2006.pdf>

A national survey, conducted by Australia’s national computer emergency response team in collaboration with the Australian Federal and State Police Forces and which analyses the computer network attack and computer misuse trends in Australia from 2005-2006.

- Australian Computer Emergency Response Team. (2008) “AusCERT Home Users Computer Security Survey,” *AusCERT*, University of Queensland. <http://www.auscert.org.au/images/AusCERT_Home_Users_Security_Survey_2008.pdf>

A national survey conducted by Australia’s national computer emergency response team that assesses the security posture of Australian-based home Internet users, their level of security awareness and attitudes to Internet security.

- Choo, K.R., Smith, R.G. and McCusker, R. (2007) “Future directions in technology-enabled crime: 2007–09,” *Australian Institute of Criminology,* Research and Public Policy Series, No. 78. <http://www.aic.gov.au/documents/9/3/6/%7B936C8901-37B3-4175-B3EE-97EF27103D69%7Drpp78.pdf>

The report examines the use of information and communications technologies in Australia and how this environment will give rise to new forms of illegality and criminality. It provides a an overall coverage of various technology-enabled crimes including unauthorised access, malware, intellectual property infringement, child exploitation, transnational organised crime and terrorism amongst others. It also discusses potential sources of risk from e-commerce and outsourcing to wireless technologies and biometric passports whilst providing a summary of existing legislation in area of cybercrime and touches upon criminal defences, jurisdictional issues, sentencing and punishment and law enforcement in the arena of Australian cybercrime.

- McAfee, “A Good Decade for Cybercrime McAfee’s Look Back at Ten Years of Cybercrime,” *McAfee Inc.,* <http://www.mcafee.com/us/resources/reports/rp-good-decade-for-cybercrime.pdf>

A brief report discussing the various stages of cybercrime from 2000-2010 and outlining the top 5 exploits and top 5 scams which have marked the decade. There is a useful glossary at the end which covers the definitions of some key terms in the cybercrime context.

- The Parliament of the Commonwealth of Australia, “Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime - The Report of the Inquiry into Cyber Crime”, *House of Representatives Standing Committee on Communication*s, June 2010, Canberra. <http://www.aph.gov.au/house/committee/coms/cybercrime/report/full_report.pdf>

A comprehensive report based on an inquiry into the incidence and impact of cyber crime on Australian consumers and the Australian economy with an examination of the adequacy of Australia’s measures to combat the problem, including a set of recommendations for improvement.