Background Note

Security

The expansion of the Internet has opened up many new opportunities for criminals to exploit online vulnerabilities, leading to an expansion of cybercrime.

Cybersecurity is generally understood to include security threats to countries, companies and individuals as Internet users, and to the Internet itself. It includes protection of information against its unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. At the centre of the debate to enhance cybersecurity are issues of greater collaboration across countries and questions of authentication and identification.

Attacks to one country's critical infrastructure have also attracted international attention. In April and May this year, a sophisticated Internet attack on Estonia's digital infrastructure, probably through distributed denial-of-service attacks (DDoS), paralyzed large parts of the country's websites.

Cyberthreats include spam, spyware, botnets, viruses and other malware and techniques (such as phishing) which may lead to fraud, identity theft, breaches of privacy and other risks associated with online transactions.

Spyware is computer software that is installed surreptitiously on a personal computer to intercept or partially control the computer, without the user's knowledge and consent. A botnet is a number of computers that, although their owners are unaware of it, have been set up to forward transmissions – including spam or viruses – to other computers on the Internet. Phishing is sending an e-mail to a user falsely claiming to be a legitimate business, in an attempt to scam the user into surrendering private information that will be used for identity theft or other frauds.

Business is especially concerned about cybersecurity, which involves the security of transactions on the Internet and the confidence that users need in order to do business on the Internet.

The cross-border nature of cybercrime makes dealing with it difficult. Many organizations have created Computer Security Incident Response Teams, which provide rapid notification of security incidents and adopt measures against current and future threats.

The problem requires international cooperation and international response mechanisms, like the Council of Europe's Cybercrime Convention and the Forum of Incident and Security Teams (FIRST), the leading international body for incident response, which now gathers more than 180 organizations from around the world.

* * *

Issued by the United Nations Department of Public Information - DPI/2477B - November 2007