Comment internet favorise la cybercriminalité ?





La criminalité moderne étalonne son emprise par une panoplie de forfaits réalisés par le biais du Réseau Internet. On peut citer entre autre les escroqueries, les fraudes, le harcèlement, les conflits, les espionnages, le vandalisme, le piratage informatique.

La cybercriminalité contient l’ensemble des activités illégales, irrégulière commis dans le cyberespace. En outre, elle recouvre toute forme de malveillance électronique réalisée au moyen de l’informatique et des télécommunications, à savoir la téléphonie, et les cartes à puce. On assiste donc à une nouvelle forme de criminalité dont l’ampleur est considérable et les dégâts encore indéchiffrés appelant ainsi la société et tous les Gouvernements et associations à se mobiliser contre ce fléau. La question pertinente est : comment ? En tant que spécialiste Anti cyber Criminalité, j’ai pu identifier d’éventuelles solutions, mais avant il convient de préciser en profondeur le contexte ainsi que les enjeux de la Cybercriminalité.

Les technologies de la communication et de l’information sont devenues la proie de malintentionnées (vol d’ordinateurs ou de données, otage de ressources informatiques,…). Le web est une proie facile dont l’extension vise surtout la criminalité financière, ainsi naît de nouveaux délits : fraudes informatiques, piratage de logiciels…). La virtualisation des services et des transactions, la possibilité d’agir à distance et de plus sous de fausses identités ou pire des identités usurpées, de se servir d’un grand nombre d’outils techniques (serveurs, fournisseurs d’accès internet, etc.). Tous ces facteurs favorisent des formes d’organisations, d’échanges et d’activités criminelles très profitables au regard de l’investissement et du risque encouru.

D’autres parts, dans le cyberespace, la communication quel que soit la distance, le moment, est rendue possible. Quant aux utilisateurs ils proviennent de toutes les classes d’âges, des enfants aux plus âgés, toutes les classes sociales, la classe sociale moyenne, la haute classe sociale. Tous côtoient virtuellement des cybercriminels de diverses origines et de toutes sortes, les escrocs professionnels, les délinquants, les criminels, les terroristes. Dès lors le cyberespace représente un espace potentiellement dangereux ou les abus sont omniprésents et permanents.

Un autre aspect de la cybercriminalité est ce que j’ai nommé « La Cybercriminalité Politique ». Une forme naissante de crime contre l’Humanité encore négligé par les Institutions Internationales. L’opinion peut être manipulée, endoctriner, la circulation de rumeurs facilitée, l’espionnage, la déstabilisation sociale.

Le réseau internet est certes un outil indispensable et généreux, mais se borner les yeux quant aux dangers encourus dans le cyberespace relèverait d’une irresponsabilité.

Quelles solutions ?

L’erreur majeure commise est de sensibiliser uniquement la population sur la sécurité informatique, ou encore de fournir des précautions élémentaires, l’on se doit de faire comprendre les fondements et l’organisation du système qu’ils utilisent. L’efficacité de cette lutte repose également sur une approche ambivalente c’est-à-dire préventive et curative. Autrement exprimé il sera question d’accroître la difficulté des attaques en minimisant les risques pour les utilisateurs. Ainsi les infrastructures informatiques et celles des télécommunications à travers des mesures de sécurité techniques, procédurales, managériales et incontrôlable en totalité par les cybercriminels doivent être renforcées. Aussi une volonté politique doit être engagée, et ce au plan national et international. Il faut également mettre en place des systèmes juridiques sévères et renforcée par l’intervention d’autorités internationales. Les pays exemptés de lois contre la cybercriminalité constitue une terre promise pour les cybercriminels.

A la lumière des potentiels dangers encourus, une lutte permanente comparable à celle des guerres mondiales, des crises économiques, et du réchauffement climatiques, doivent être l’objet de sommets et de débats politiques. Certes le Sommet mondial sur la société de l’Information, tenu à Genève en 2003 et à Tunis en 2005, a notamment contribuer à identifier la nécessité d’une Gouvernance de l’Internet plus Internationale, plus « onusienne », et la nécessité d’un internet plus fiable et plus accessible à l’ensemble de l’Humanité.

Mais une identification n’est pas suffisante, il faut également prendre des mesures concrètes. Pour ma part il conviendrait de créer des Filières Spécialisées dans le domaine de la Cybercriminalité. Soit dit en passant la Cybercriminalité ne se rattache pas seulement au piratage informatique. Les cybercriminels sont devenus des experts combinant des connaissances psychologiques, informatiques, d’ordres techniques pour atteindre leur fin. A titre illustratif l’on pourrait citer la Cybercriminalité en Afrique de l’Ouest, domaine ou ma spécialité est plus accrue. En effet les cybercriminels de cette région usent du manque affectif de certaines personnes riches pour notamment leur extorquer de l’argent ou d’autres biens. Ainsi des expertises doivent être menées dans ce domaine et entrainé des applications pratiques pour enfreindre ce phénomène. Quant aux utilisateurs néophytes du Réseau Internet, il leur faut se tenir vigilent quant à l’emploi d’Internet et maîtriser les actions qu’ils y entreprennent et enfin et surtout se mettre au parfum de l’actualité concernant la Cybercriminalité.

Aujourd’hui, il existe différents types de communication :

* La tradition orale
* La gestuelle
* L’écriture
* Les images
* Etc….

Mais la plus utilisée aujourd’hui est la communication virtuelle via internet et divers réseaux sociaux.