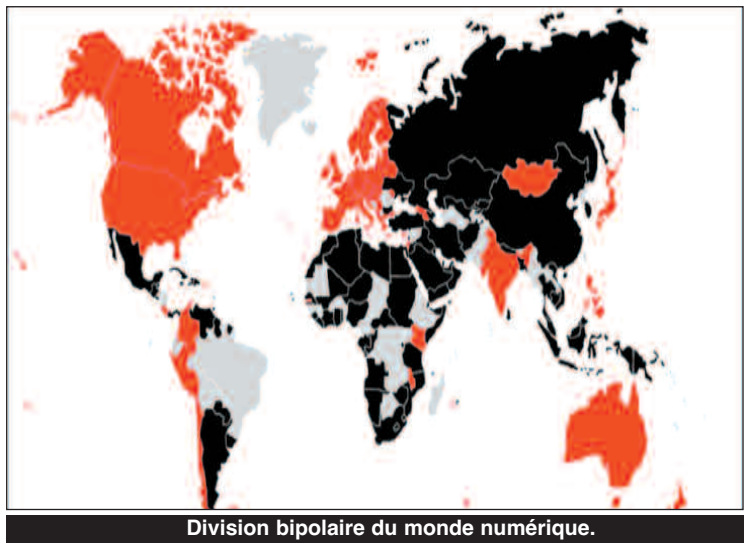
Prévisions sur les risques Internet en 2013

Les mois de décembre et janvier sont ceux des bilans et prévisions. Cette contribution portera sur les éléments que je considère parmi les plus importants du bilan 2012 de la cybersécurité et les prévisions pour 2013. Plus précisément sur les risques et menaces que les utilisateurs des ordinateurs, dont les citoyens ordinaires, encourent en 2013 à un moment où des décisions les concernant, comme la consultation des comptes CCP et le paiement de factures par téléphone portable, le lancement imminent de la 3G et la démocratisation de l'internet sont annoncées.



Division bipolaire du monde numérique.

Exemples de cyberattaques en 2012 :

23 avril 2012 : L'Iran déconnecte de l'Internet ses installations de l'industrie pétrolière, selon ses responsables, suite à une série de cyberattaques ayant ciblé les systèmes informatiques du secteur.

28 mai 2012 : Découverte au Moyen- Orient dans des milliers d'ordinateurs appartenant à des entreprises et institutions du très sophistiqué malware (virus) Flame, développé sans aucun doute par un Etat à des fins de cyberespionnage : assemblage et vol de données, modification à distance des paramètres des ordinateurs, enregistrement des conversations, etc. Flame est programmé pour effacer toute trace de son intrusion le rendant difficilement détectable et pour s'autodétruire une fois sa mission achevée.

5 juillet 2012 : Cyberattaques menées par l'organisation Anonymous contre des ordinateurs appartenant à personnalités politiques syriennes, des ministères et des sociétés syriennes et vol de 2,4 millions d'emails.

19 août 2012 : Cyberattaques en Inde contre 80 sites internet et contre les réseaux SMS de téléphonie mobile, suivies par la publication de photos de massacres et des envois massifs de SMS pour la propagation d'une rumeur relative à des massacres d'immigrants dans le nord-est du pays.

La cyberopération a provoqué une panique au sein des immigrants qui ont voulu quitter le pays massivement. Conséquences : 90 morts, 400 000 personnes déplacées.

12 août 2012 : Cyberattaque contre 30 000 ordinateurs de l'une des plus importantes compagnies pétrolières du monde, la Saudi Arabian Oil Co, visant certainement à nuire à l'économie de l'Arabie Saoudite. C'est la cyberattaque la plus importante de l'histoire dirigée contre un seul objectif économique.

21 septembre 2012 : Cyberattaques contre des banques américaines dont JPMorgan, Chase et Bank of America provoquant d'importantes perturbations.

21 septembre 2012 : Découverte par l'Agence nationale de la sécurité systèmes d'information (Anssi) que les ordinateurs des collaborateurs à l'Elysée de l'ancien président français Sarkozy étaient victimes d'intrusions par le malware Flame depuis des mois.

L'opération a conduit certainement au vol d'informations confidentielles concernant la politique du gouvernement français.

26 décembre 2012 : Cyberattaque ciblant les réseaux informatiques d'une centrale électrique et d'autres industries dans le sud de l'Iran par le désormais célèbre malware Stuxnet, selon un responsable de la Défense civile iranienne. Ces exemples, qui ne représentent qu'une infime partie des cyberattaques survenues en 2012 et qui continueront en 2013, mettent en évidence qu'aucun citoyen, secteur ou pays ne sont à l'abri de la cybermenace comme cette autre menace globale qui est le terrorisme. L'Algérie a été parmi les précurseurs pour la mise en place d'une stratégie de confrontation du terrorisme et de sensibilisation aussi bien de ses citoyens que de ses partenaires étrangers, ce qui ne semble pas être le cas pour la cybermenace.

Saut spectaculaire du développement des malwares en 2012 :

Les milieux de la cybercriminalité sont à l'origine d'un développement qualitatif et quantitatif si rapide de malwares qu'il paraît impossible en 2013 pour les sociétés de sécurité informatique de découvrir et de développer suffisamment et surtout à temps des antivirus.

A la fin de 2012, il y avait déjà 85 millions de malwares. Les données suivantes donnent une idée de l'évolution de cette rapide croissance : 74 000 malwares sont développés par jour en 2011 dans le monde par les cybercriminels et les Etats contre 100 000 en 2012.

Deux autres constations importantes s'imposent :

- la proportion des malwares du type Trojan Horse (Cheval de Troie) servant au vol d'informations personnelles et professionnelles ne cesse de croître. Les Trojan Horse représentent aujourd'hui 70% des malwares développés ;

- mêmes constations concernant les malwares destinés à la technologie installée sur les smartphones comme l'Androïde Google, Apple (iPhone), Nokia, Samsung, BlackBerry, etc. Selon Kaspersky, plus de 35 000 malwares destinés aux Androïdes ont été identifiés fin 2012, soit 6 fois plus qu'en 2011. Cette croissance en exponentielle se maintiendra en 2013.

Devant cette situation et à la veille de l'introduction de la 3G en Algérie, quelles stratégies, mesures de protection et de prévention comptent prendre les opérateurs de la téléphonie mobile, les ISP (Internet Service Provider) et aussi le gouvernement pour protéger les citoyens et les institutions ?

Les citoyens sont les plus vulnérables aux cyberintrusions, aux escroqueries et aux arnaques sur l'internet, comme le vol des informations personnelles ou celles du type «loterie nigériane» ou d'escroquerie «419» dont l'objectif est d'amener la victime à accepter de verser une participation financière pour régler des soi-disant frais de dossiers pour permettre l'envoi de millions d'euros à son profit.

Les spécificités des cyberrisques pour 2013 :

- développement de malwares par les cybercriminels plus rapide que le développement d'antivirus par les sociétés de sécurité informatiques ;

- amélioration continue de la sophistication des cyberarmes et baisse du niveau de connaissance nécessaire pour les utiliser. Il n'est plus nécessaire d'être informaticien pour utiliser une cyberarme, comme on n'a pas besoin d'être mécanicien pour conduire une voiture ;

- lenteurs dans la mise en place de stratégies par les gouvernements pour contrer la cybermenace ;

- les lois actuelles ne sont pas adaptées à la cybermenace et n'ont pas un effet dissuasif. Une situation qui rappelle celle du terrorisme durant les années 1990 ;

- disponibilité des cyberarmes sur l'internet gratuitement ou pour une vente libre, alors qu'il faut une autorisation pour acheter un fusil de chasse ;

- il est très difficile sinon impossible d'identifier et de localiser un utilisateur des cyberarmes. Des outils existant sur l'internet permettent l'anonymat.

Sophistication, facilité d'emploi, disponibilité pour des sommes modiques ou gratuitement, des caractéristiques qui pourraient intéresser les milieux terroristes et préoccuper les services de sécurité.

Le préjudice financier de la cybercriminalité en 2013 :

Le préjudice financier causé par la cybercriminalité à des internautes adultes dans 24 pays seulement s'élève à 388 milliards de dollars en 2010. Le marché global du trafic de drogue s'élève quant à lui à 411 milliards de dollars. La cybercriminalité rapporte plus que le trafic mondial des drogues de marijuana, de cocaïne et d'héroïne combinées. La valeur et le préjudice des informations confidentielles volées n'ont pas été pris en considération. Les informations confidentielles sont-elles quantifiables d'ailleurs ?

Cette tendance persistera en 2013, si bien que des pays ont fait de la lutte contre la cybercriminalité une priorité nationale au même titre que la lutte contre le terrorisme.

Militarisation de l'internet et la cyberguerre en 2013 :

A cause du coût réduit, l'efficacité, la facilité de déploiement et l'anonymat, les cyberarmes constituent des armes idéales en quelque sorte ; aucun pays ne peut continuer à les ignorer car elles conduisent à réduire les capacités de résistance de l'ennemi avant le combat ou les attaques avec les armes conventionnelles. Des pays investiront fortement en 2013 dans le développement de cyberarmes (Botnets et malwares du type Advanced Persistent Threat ou APT) pour s'offrir des capacités offensives et dissuasives de cybersécurité.

La cyberguerre cible en priorité les infrastructures militaires et celles civiles dites sensibles comme le montrent les quelques exemples de cyberattaques de 2012 cités plus haut. En 2013, la cyberguerre connaîtra un développement, les Etats dépenseront plus pour les cyberarmes pour en faire aussi des armes de destruction. Les cyberarmes vont-elles se transformer d'armes d'interruptions massives (Weapons of Mass Interruption) en armes de destruction ?

Conscient de cette situation, l'Iran, à titre d'exemple, a organisé en décembre 2012 un exercice simulant des cyberattaques contre les réseaux informatiques militaires et civils des infrastructures sensibles dont ceux des hydrocarbures, des banques et des sites nucléaires.

L'année 2013 sera-t-elle de la cyberguerre entre nations ?

Hacktivisme :

Le hacktivisme consiste en l'utilisation des outils légaux (réseaux sociaux) et illégaux (intrusion dans les réseaux et emploi des cyberarmes) de l'internet à des fins d'expressions politiques anonymes, de protestations sociales et politiques. Le hacktivisme a été, en 2012, la principale préoccupation des experts en sécurité informatique suivis par les activités des cybercriminels et enfin les cyberattaques dont les Etats seraient à l'origine. 2013 connaîtra une intensification du hacktivisme d'organisations comme Anonymous dans un but de contestation sociale ou politique. Début janvier 2013, Anonymous a mis en ligne une pétition demandant que les cyberattaques du type DDoS (Déni de Services) soient reconnues officiellement comme une forme de protestation et non un crime.

Ces organisations supposées précédemment apolitiques pourraient se convertir en cyberespions professionnels ou cybermercenaires au profit de parties occultes.

L'internet :

Les 150 représentants de pays sur les 193 membres qui se sont réunis à Dubaï en décembre sous les auspices de l'Union internationale des télécommunications, Organisation des Nations unies, n'ont pas réussi à se mettre d'accord sur les mises à jour du Traité de 1988 sur les télécommunications internationales à cause de l'internet (ma contribution sur *le Soir d'Algérie* du 5 décembre 2012).

Elle s'est achevée par la signature par 89 pays seulement du document final dont la Russie, la Chine, plusieurs pays africains et arabes dont l'Arabie Saoudite, Qatar, Egypte, Tunisie, Maroc et l'Algérie. Certains ont émis des réserves pour préserver leurs intérêts futurs. Les réserves ont en général porté sur le droit de sauvegarde des intérêts nationaux, à ne pas reconnaître les mesures prises par des gouvernements et pouvant compromettre le fonctionnement de leurs propres services de télécommunication.

La presque totalité des pays occidentaux ont refusé de signer.

Le monde numérique semble divisé en deux, rappelant ainsi le bipolarisme de la guerre froide.

La raison est que le traité qui ne se réfère pas directement à l'internet a touché des domaines regardant néanmoins l'internet : les spams et la sécurité des réseaux de télécommunication internationaux. Les pays non signataires ont trouvé ces deux dispositions trop vagues et comme une recommandation pour les Etats à surveiller les utilisateurs de l'internet. Il est clair que des pays sont venus à la WCIT pour légitimer des pratiques de surveillance et de censure qu'ils pratiquent déjà, et les autres avec l'objectif de maintenir le Traité de télécommunication inchangé et empêcher qu'ils puissent affecter l'internet.

Par Abdelaziz Derdouri*

En 2013, plusieurs rencontres internationales sur les technologies de l'information sont déjà programmées, il est très peu probable sinon impossible qu'elles puissent aboutir sur un accord tellement les intérêts sont contradictoires : World Summit on the Information Society, World Telecommunication Policy Forum, Internet Governance Forum.

Conclusion

Quelques pays ont élevé la cybermenace au rang des menaces principales comme le terrorisme à cause des préjudices qui peuvent être causés aux citoyens et aux institutions. L'année 2013 sera-elle celle de la prise de conscience de la cybermenace ? L'Algérie est classée parmi les pays les plus infectés dans le monde à cause de l'utilisation de logiciels qui sont des contrefaçons et le téléchargement de ceux gratuits contenants des malwares. La faute en incombe principalement au manque de mesures de sensibilisation. Des pays et parfois des opérateurs organisent des campagnes périodiques de sensibilisation au profit des citoyens dont la durée varie d'un mois à une semaine, c'est le cas des Etats-Unis, le Canada, le Sri Lanka, la Côte d'Ivoire, l'Union européenne, Google, etc.

La Malaisie en a organisé une campagne ayant pour thème : «La sécurité informatique, c'est la responsabilité de tous». Mettant en évidence le rôle du gouvernement et celui du citoyen dans la cyber-sécurité, rôle qui ne peut être joué par ce dernier sans l'organisation de campagnes de sensibilisation et d'éducation. En général, une bonne politique de sécurité commence en premier par la prise en charge sérieuse de l'aspect humain : formation et sensibilisation, et il ne sert à rien d'acquérir des équipements coûteux contre la cybermenace sans ce préalable. Malgré l'utilisation d'équipements les plus modernes du monde, les Etats-Unis n'ont pas pu éviter WikiLeaks, qui est dû à une défaillance humaine. L'année 2013 est une année qui va faire mal dans le monde et l'Algérie n'est pas dans la meilleure position car la seule chose pire que l'insécurité est un faux sentiment de sécurité.

A. D.

*** Officier supérieur en retraite. Directeur d'une société de sécurisation des réseaux. Enseignant de cybersécurité à l'Ecole nationale supérieure de sciences politiques, Alger.**