TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION (TIC)

Une loi sur la

Par Abdelaziz Derdouri
Officier supérieur en retraite

Introduction

Partons du constat selon lequel les technologies de l'information et de la communication (TIC) se développent non seulement à un rythme infiniment plus rapide que les réformes juridiques, mais qu'elles évoluent également dans un environnement marqué par un «vide juridique», car les lois existantes ne sont plus pertinentes. Cela nous conduit à une situation paradoxale dans la mesure où les règles afférentes au fonctionnement des TIC sont définies et imposées, non pas par l'Etat, mais par des acteurs nationaux et étrangers dominant le secteur, ainsi que par les cybercriminels.

La première question qui se pose donc est de savoir si les TIC en Algérie sont vouées à poursuivre leur développement en dehors de tout contrôle légal effectif, au détriment de la sécurité et intérêts nationaux, car les institutions juridiques et législatives ont une longueur de retard sur les technologies et la perception de la cybermenace. Chaque Algérien dépend de plus en plus directement ou indirectement des systèmes et des réseaux d'informations. Ces derniers constituent l'épine dorsale de l'économie, de la sécurité nationale et aussi des activités quotidiennes des citoyens. Cette dépendance n'est un secret pour personne et risque d'être exploitée pour affaiblir et déstabiliser le pays.

Des voix préoccupées se sont déjà fait entendre au sujet de la nécessaire protection des réseaux. Les citoyens s'inquiètent également de la multiplication des cyberattaques dont ils sont victimes. Elles sont en augmentation constante et leurs fréquences et sophistication sont sans précédent. Elles se répandent vers tous les secteurs de l'économie, les secteurs stratégiques, les industries, les services, les citoyens… Elles ne connaissent pas de frontières géographiques. Parmi les nombreuses mesures visant à protéger contre cette menace, une loi, car la cybersécurité est aussi une affaire juridique. En effet, une loi sur la cybersécurité comprendrait de nombreux avantages qu'il ne faut pas sous-estimer. Des études ont montré qu'une telle loi contribuerait à réglementer le secteur des TIC, à renfoncer l'autorité, à dissuader les cybercriminels et permettrait aussi une meilleure protection des infrastructures sensibles. Ces dernières, comme les secteurs de l'énergie électrique, de l'eau, du transport, des finances, des TIC, etc., essentiels à l'activité du pays, sont ciblées régulièrement dans un objectif d'interrompre ces services et causer des préjudices.

Les activités de cyberespionnage et de cybercriminalité contre l'Algérie sont réelles. Elles ont non seulement commencé, mais les experts prévoient que leur nombre, persistance et gravité continueront à augmenter au cours des prochaines années.

Persévérance des cyberattaques contre l'Algérie

En ce début d'année 2015, d'autres attaques contre l'Algérie et les Algériens ont été rendues publiques. Des opérations de cyberespionnage de l'«Equation Group», utilisant le virus de cyberespionnage le plus dangereux jamais découvert, n'ont été découvertes que récemment alors qu'elles ont débuté depuis des années. Ses victimes tombent généralement dans les catégories suivantes : gouvernement, Défense, Energie et Finances.

Le groupe «Desert Falcons» pratiquait lui aussi le cyberespionnage ciblant des organisations de haut profil, des personnalités politiques, des fonctionnaires chargés de la lutte contre le blanchiment d'argent et ceux en possession d'informations géopolitiques importantes. Ses victimes sont localisées dans de nombreux pays dont l'Algérie.

Une série de maliciels, Babar, Bunny, Casper, Dino, NBot et Tafacalou, dont la création est attribuée aux services de renseignement français par au moins trois grandes compagnies de sécurité informatique américaines et européennes, ont été utilisés pour voler des données appartenant à des organisations gouvernementales et entreprises de plusieurs pays dont l'Algérie.

Enfin l'attaque la plus récente, et fait particulier en Algérie, concerne une entreprise économique du secteur privé. Toutes ces attaques ne semblent pas avoir suscité de réactions à la hauteur des enjeux par manque de cadre juridique et organisationnel adapté à la cybersécurité.

Une loi sur la cybersécurité ?

Il n'existe pas encore de critères précis et clairs pour déterminer si une cyberattaque est un acte criminel, un acte d'hacktivisme, de terrorisme ou simplement l'utilisation de la force par un Etat dans le cyberespace. Quel serait donc l'impact d'une loi si ce dernier est en permanente évolution et où de nombreux acteurs étatiques et non étatiques opèrent dans le secret ?

Une loi sur la cybersécurité ne peut pas être considérée comme une fin en soi, ni constituer une disposition globale, mais elle permettrait de compléter les dispositions protectrices et préventives conférées par d'autres textes déjà existants. Elle permettrait de lutter plus efficacement contre, par exemple, l'acquisition des cyberarmes (Botnet, DDoS, etc.) qui ne sont définies dans aucun texte de loi algérien et qui sont aujourd'hui commercialisées librement dans le Darknet alors qu'il faut une autorisation pour acquérir un simple fusil de chasse. Cette loi pourrait aussi rendre illégaux la vente et l'achat des logiciels espions (spyware), la commercialisation des données volées ou la mise en place de n'importe quel dispositif technologique pour localiser, écouter, surveiller ou installer une webcam ou toute autre forme de périphérique de surveillance à l'insu de la cible, sans autorisation préalable de la justice, etc. A titre d'exemple, le Président américain, Barack Obama, a signé le 2 avril 2015 un nouveau décret complétant la loi américaine, visant à imposer «des sanctions aux personnes ou entités» nationales et étrangères qui se livrent à des cyberattaques menaçant «la sécurité nationale, la politique étrangère, l'économique ou la stabilité financière des Etats-Unis».

Les lois de cybersécurité prévoient la mise en place d'une organisation nationale de cybersécurité qui décrit les responsabilités des différents organismes de cybersécurité, leurs prérogatives, les mesures de coordination, de prévention et de gestion des incidents. Le but de la loi sur la cybersécurité est donc de forcer les gouvernements, les organisations et les entreprises à prendre les mesures pour protéger les systèmes et les données contre les cyberattaques.

Qui est réellement responsable de la cybersécurité ?

La cybersécurité doit être abordée comme un problème de gestion des risques à l'échelle des plus hauts responsables et non pas seulement comme un problème informatique. Son évaluation doit prendre en considération l'écosystème le plus large possible. Elle est abordée lors des réunions du gouvernement et du conseil d'administration au même titre que les autres questions stratégiques. Elle n'est pas seulement une question de «verrouillage», prévention ou d'équipements, mais aussi de culture. Une question d'éducation, de sensibilisation et de responsabilisation individuelle. La sécurité doit être une culture intégrée au sein des organisations et seuls une loi et le premier responsable d'une organisation peuvent mettre en place cette culture et la parrainer.

Responsabilités du gouvernement

En plus d'exiger du gouvernement de prendre des mesures pour protéger les infrastructures sensibles et d'offrir un soutien pour stimuler la cybersécurité, la loi sur la cybersécurité obligerait les entreprises à prendre des mesures volontaires pour améliorer la défense des réseaux, à coopérer avec le gouvernement pour la mise en œuvre de mesures pertinentes et de se soumettre aux contrôles relatifs au respect des normes mises en place (Standards). Beaucoup de pays ont créé une autorité gouvernementale au niveau de la chefferie du gouvernement ou de la Présidence qui centralise toutes les décisions liées à la cybersécurité. Le gouvernement organiserait et coordonnerait la coopération entre les institutions compétentes en matière de cybersécurité et définirait clairement les responsabilités afin de lutter contrer les cyberattaques qui affectent la sécurité nationale.

Il définirait et soutiendrait les mesures pour améliorer les compétences de ceux qui travaillent dans le domaine de la cybersécurité, la création de pôles de Recherche et Développement (R&D) et la définition d'un programme national unique d'enseignement de la cybersécurité dans les universités. Les étudiants sélectionnés sur la base d'un concours dont l'un des critères serait un engagement pour l'amélioration des moyens de cyberdéfense de la nation (cas de la loi américaine). Les outils de cybersécurité utilisés pour protéger les réseaux en Algérie sont étrangers, il faut savoir qu'il n'y a de sécurité réelle que si l'origine des outils et des solutions de sécurité est nationale. Enfin (last but not least), le gouvernement élabore et met en œuvre une stratégie nationale de cybersécurité, qui doit comprendre une vision à long terme et qui englobe tous les aspects de la sécurité nationale. La loi sur la cybersécurité est une partie intégrante de cette stratégie.

Beaucoup de pays ont créé une autorité gouvernementale au niveau de la chefferie du gouvernement ou de la Présidence qui centralise toutes les décisions liées à la cybersécurité. Le gouvernement organiserait et coordonnerait la coopération entre les institutions compétentes en matière de cybersécurité et définirait clairement les responsabilités afin de lutter contrer les cyberattaques qui affectent la sécurité nationale.

Les organismes de contrôle

Ces organismes assurent la fonction d'autorité nationale de sécurité. Ils définissent les mesures techniques et organisationnelles de défense et de protection et sont chargés aussi des contrôles et inspections des systèmes d'information des infrastructures sensibles. Le Royaume-Uni a créé le «Centre for the Protection of National Infrastructure (CPNI)», une autorité gouvernementale qui fournit des conseils de sécurité aux entreprises et organisations. Aux Etats-Unis, la loi sur la cybersécurité impose au gouvernement de faire établir des normes uniformes (standards) en matière de cybersécurité par le NIST (National Institut of Standards and Technology), d'analyser les attaques et de tirer des enseignements (loi japonaise de cybersécurité). Le NIST établit des normes de cybersécurité mesurables et vérifiables en ce qui concerne la sécurité des logiciels et élabore un processus permettant de vérifier la conformité (compliance) des organisations.

Habilitation des prestataires de services ou prestataires de confiance

Les lois existantes exigent de veiller à la sécurité lorsqu'il est fait appel à la prestation par des tiers. Toute prestation dans le domaine des systèmes d'information doit être encadrée par des clauses de sécurité. Ces clauses spécifient les critères et les mesures que le prestataire doit respecter dans le cadre de ses activités, et les infrastructures sensibles ne peuvent faire appel qu'à des prestataires habilités et de confiance.

Au Royaume-Uni la liste de ces prestataires est établie par le GCHQ (Government Communications Headquarters), un service de renseignement et de sécurité. Ces prestataires peuvent intervenir dans le cadre de la protection contre les cyber-attaques et peuvent être aussi chargés du «nettoyage» des réseaux après les cyberattaques réussies contre les entreprises du Royaume-Uni.

En France, les prestataires d'évaluation de sécurité (audit) des systèmes de l'information sont agréés par le Premier ministre dont dépend le comité directeur de la certification en sécurité des technologies de l'information. Aux Etats-Unis, les textes sont plus directs et plus clairs (CyberSecurity Act of 2010), seules les compagnies américaines sont habilitées et certifiées et il est illégal d'employer des experts étrangers dans le secteur de la cybersécurité. La loi américaine va plus loin, puisqu'elle prévoit que seules les compagnies américaines peuvent être fournisseur d'accès internet (IPS) au profit des institutions gouvernementales et des infrastructures sensibles.

Obligation de déclarer les cyberattaques

Une loi sur la cybersécurité devrait exiger des organisations publiques et privées de rapporter ou notifier à un organisme gouvernemental les attaques dont leurs réseaux ont été victimes. Dans la majorité des pays cet organisme est le CERT (Computer Emergency Response Team).

Des mécanismes plus ou moins similaires sur le recueil d'informations et leur diffusion ont été mis en place dans le cadre de la lutte antiterroriste en Algérie. Il suffirait de s'inspirer de ces mécanismes et de les adapter. Après une attaque, une enquête devrait être diligentée aussi par une commission gouvernementale d'analystes (Cyber Security Forensic Analyst) pour déterminer les maliciels utilisés, les vulnérabilités exploitées, tirer des enseignements