Stratégie multidimensionnelle de cyberdéfense à l'ère d'Internet des Objets

Professeur Yacine CHALLAL

Ecole nationale Supérieure d'Informatique Laboratoire de Méthodes de Conception de Systèmes

Résumé

«Internet des Objets (IdO)» est une évolution majeure qui s'inscrit dans la continuité des développements récents des technologies de l'information et de la communication et des systèmes embarqués. Cette évolution sera accompagnée d'une évolution de l'écosystème technologique environnant dans toute sa complexité. L'IdO suscitera des questions, qui concerneront directement la sécurité des biens et des personnes. Par exemple, certaines applications peuvent être étroitement liées à des infrastructures stratégiques telles que la fourniture d'eau et d'électricité, la surveillance de ponts et bâtiments, tandis que d'autres géreront des informations liées à la vie privée des personnes comme leurs déplacements et états de santé. Devant cette menace globale, les pouvoirs publics devraient élaborer une stratégie de cyberdéfense multidimensionnelle.

Mots-clés: Internet des Objet, Stratégie multidimensionnelle, cyberdéfense

Introduction

Internet des objets (IdO) est une évolution majeure qui s'inscrit dans la continuité des développements récents des technologies de l'information et de la communication et des systèmes embarqués. Cette évolution sera accompagnée d'une évolution de

l'écosystème technologique environnant dans toute sa complexité. En effet, comme illustré par la Figure 1, le réseau mondial Internet a évolué ces dernières décennies, d'un réseau de calculateurs à un réseau d'ordinateurs personnels, puis vers un réseau qui intègre tout dispositif communiquant : les tags RFID, les réseaux de capteurs et actionneurs, les réseaux véhiculaires, etc. A cette ère de la connectivité globale et d'Internet des objets, plusieurs défis sécuritaires émergent comme de nouveaux challenges constituants un espace sécuritaire à part entière : le cyberespace, en plus des quatre espaces conventionnels des armées : la terre, la mer, l'air et l'espace.

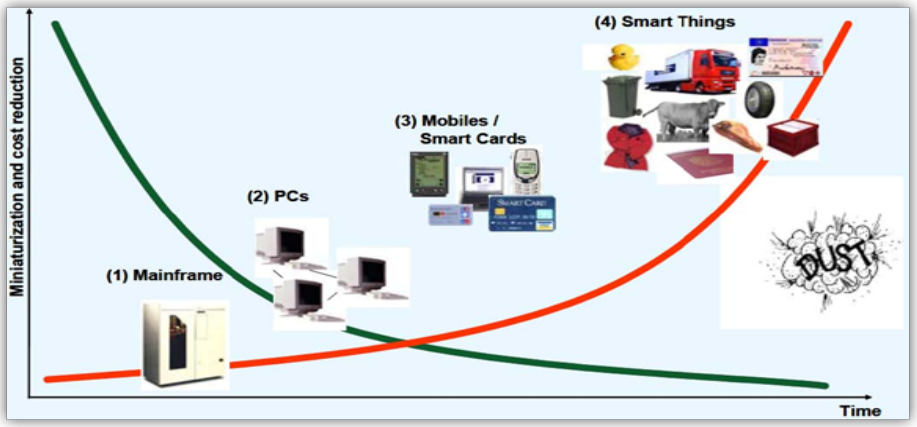

Figure 1 Evolution de notre environnement technologique. Fleisch et al.

En effet, l'internet des objets suscitera des questions, qui concerneront directement la sécurité des biens et des personnes. Par exemple, certaines applications peuvent être étroitement liées à des infrastructures stratégiques telles que la fourniture d'eau et d'électricité, la surveillance de ponts et bâtiments, tandis que d'autres géreront des informations liées à la vie privée des personnes comme leurs déplacements et états de santé.

Illustration 1: Cyberespace et Infrastructures Critiques

Le cyberespace supporte et contrôle le fonctionnement d'infrastructures critiques en lien avec des secteurs aussi sensibles que la santé, l'énergie, le transport, l'agriculture, les finances, etc.

Vu son rôle central dans les sociétés contemporaines, le cyberespace constitue en lui même une infrastructure critique requérant une protection maximale et toute l'attention des autorités publiques.

En effet, l'Union Internationale des Télécommunications (ITU) [1] définit les infrastructures critiques par « les systèmes clés, services et fonctions dont la perturbation ou la destruction aurait un impact délibéré sur la santé publique, la sécurité des personnes, le commerce et la sécurité nationale ou toute combinaison de ceux-ci ». Cette définition s'applique parfaitement au cyberespace ce qui en fait de lui une Infrastructure Critique, de surcroît, Omniprésente.

Dans cet article, nous passerons en revue les défis sécuritaires que soulèvent les derniers développements d'Internet vers un Internet des objets s'immisçant dans le contrôle d'infrastructures critiques. Nous

développerons ensuite une vision critique de la situation de l'Algérie en ce qui concerne la mise en place d'une stratégie de cyberdéfense multidimensionnelle conformément aux recommandations de l'ITU.

1 Enjeux sécuritaires d'IoT

D'après le National Intelligence Council (NIC), vers 2025 les objets d'IoT seront présents dans toutes sortes de choses qu'on utilise au quotidien comme les vêtements, les voitures, les électroménagers, verrous de portes, emballages etc. Des dizaines de milliards d'objets seront donc omniprésents y compris dans les sphères les plus intimes. Ce niveau de pénétration d'Internet augmentera malheureusement l'ampleur et l'étendue des attaques. En outre, cette convergence du monde virtuel et monde physique via des objets communicants, permettra aux dommages des attaques d'atteindre des infrastructures critiques comme des réseaux de distribution d'énergie et d'eau potable, des barrages, des véhicules et moyens de transport modernes comme le métro et le tramway, les données personnelles en lien avec la santé des personnes, leur localisation et préférences, etc.

L'Algérie n'est pas à l'abri de ces évolutions incontournables, et subit comme beaucoup d'autres pays développés et moins développés les effets néfastes d'un paysage TIC vulnérable.

1.1 Cyberespace fragile en Algérie

Kaspersky Lab Industrial Control CERT classe l'Algérie au 2ème semestre 2016 à la troisième place des pays cibles d'attaques. Par ailleurs, comme le montre la figure suivante, Kaspersky labs classe l'Algérie parmi les pays où le taux d'utilisateurs infectés est très élevé, ce qui augmente le risque d'attaques de sécurité.

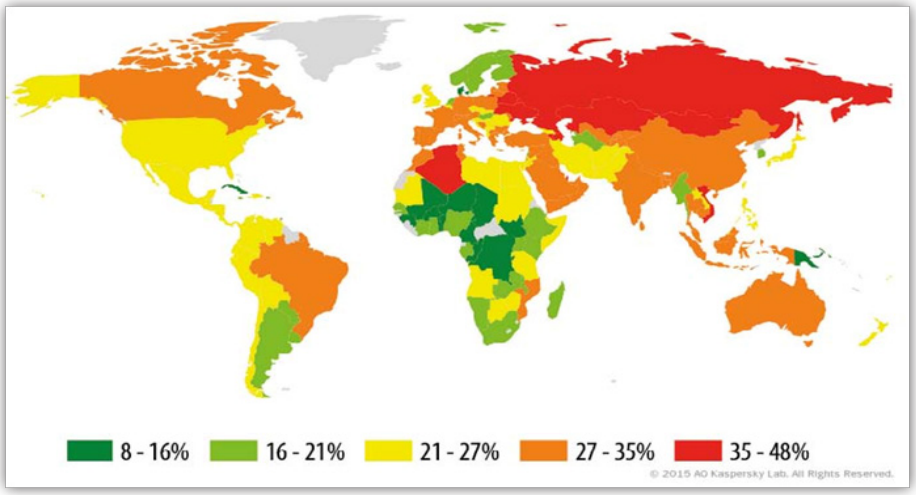

Illustration 2: Taux d'infection des utilisateurs en ligne [6]

Ce risque peut être évalué en multipliant le niveau de vulnérabilité, par la vraisemblance d'une menace par le coût des dommages engendrés en cas d'attaque.

Risque = Vulnérabilité x Menace x Coût

Dans les sections suivantes nous illustrerons l'impact des dernières évolutions vers une interconnexion de plus en plus globale, sur chacun de ces facteurs de risque.

1.2 Niveau élevé de vulnérabilité

Les Infrastructures Critiques souvent sous le contrôle d'objets connectés sont très exposées aux attaques. En effet, une protection physique des objets contrôlant ces infrastructures n'est pas envisageable pour des raisons économiques, ce qui rend leur compromission relativement facile.

Exemple : Le 21 octobre 2016, une partie d'Internet fut paralysée. Les serveurs de DYN (entreprise contrôlant une bonne partie de l'infrastructure DNS aux USA subit une attaque de déni de service

distribué (DdoS). Ceci avait causé la panne de plusieurs sites populaires (Twitter, the Guardian, Netflix, CNN, et plusieurs autres en Europe et aux USA).

Cette attaque avait été menée pour la première fois à partir d'objets connectés. En effet, pas moins de 100.000 objets compromis (dits zombies) se sont mis à attaquer les serveurs de DYN. La puissance de l'attaque a atteint pour la première fois de l'histoire les 1.2 Tera bits par seconde, ce qui représentait le double des attaques DdoS connues jusque-là.

Cette attaque illustre également la banalité des cyber-armes. En effet, ce botnet, appelé Mirai, avait infecté les 100.000 objets connectés (caméras, IP, routeurs, imprimantes, récepteurs TV, etc.) en exploitant tout simplement 68 noms d'utilisateurs et mots de passe par défaut qui n'avaient pas été modifiés par les utilisateurs de ces objets.

1.3 De nouvelles menaces

De nouvelles menaces émergent de l'inter-connectivité globale. Elles peuvent être classées comme suit :

a. Menaces amplifiées contre les données et les réseaux

L'omniprésence des objets communicants dépourvus de protection physique et de surveillance, les rendent une proie facile aux attaques matérielles et logicielles. Ces objets peuvent être volés, corrompus et contrefaits. Sans mesures particulières, les données stockées sur ces dispositifs seraient alors accessibles, y compris des données cryptographiques qui permettraient d'accéder à d'autres données sensibles ou jouer des rôles sensibles dans les systèmes complexes les hébergeant. Par ailleurs, les transmissions sans fil, sont à leur tour une proie facile à l'écoute et au déni de services

«jamming». Il existe aujourd'hui des solutions cryptographiques pour assurer des services de confidentialité, de contrôle d'intégrité, d'authentification, de non-répudiation, etc. mais beaucoup reste à faire pour rendre ces algorithmes efficaces et performants sur des dispositifs embarqués de plus en plus miniaturisés. Le CERP-IoT cite dans quelques problématiques amplifiées par la nature des objets embarqués miniaturisés. On cite notamment : l'hétérogénéité et la mobilité des objets qui rajoutent une couche de complexité aux problèmes de sécurité. La figure suivante illustre les effets de cette amplification en partant des caractéristiques d'IoT.

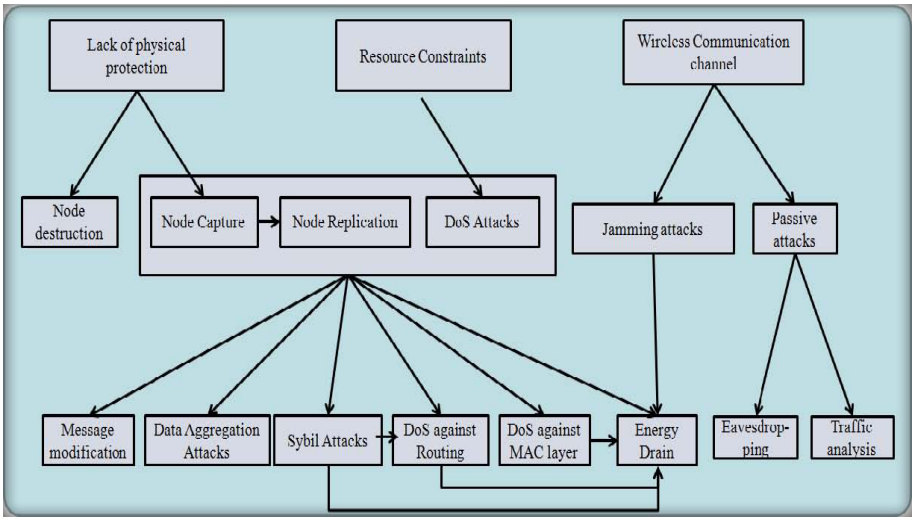

Illustration 3: Amplification des attaques contre les données et réseaux

Les fortes contraintes de ressources (CPU, mémoire, énergie) rendent la sécurisation d'IoT une tâche difficile. En effet, l'utilisation de certains algorithmes cryptographiques efficaces ne peut être réalisée sous certaines fortes contraintes, notamment énergétiques. Autrement, ces objets se verront vite leurs batteries épuisées et les applications pour lesquelles ils avaient été conçues inopérationnelles.

b. Menaces contre la vie privée

Ces dernières années plusieurs applications manipulant des données personnelles se sont développées. Ces applications stockent et traitent des données personnelles comme la localisation, les préférences personnelles (vestimentaires, alimentaires, et autres), des données en lien avec la navigation sur le web etc. Ces données collectées sont ensuite revendues à des tiers pour des fins d'analyse de données (publicité ciblée, marketing, etc). L'omniprésence des objets connectés rend cette collecte encore plus abondante et présente une menace contre ces données personnelles collectées souvent sans consentement des utilisateurs. De ce fait, il est nécessaire de légiférer à travers une loi sur la protection des données personnelles instaurant le principe d'obligation de déclaration de tout système de traitement de données personnelles et de déni par défaut de collecte de celles-ci sans consentement des utilisateurs. Par ailleurs, étant donné les volumes extraordinaires des données collectées par IoT, leur vélocité et leur variété (Big Data), des techniques de data mining préservant l'information sensible (PPDM : Privacy Preserving Data Mining) doivent être développées.

c. Menaces contre le monde physique

De nouvelles menaces inégalées pèsent aujourd'hui sur les systèmes connectés via des objets vulnérables. Les dommages en cas d'attaque atteignent directement les personnes et leurs biens. De ce fait, il est nécessaire de développer une approche systémique de la cyberdéfense tenant en compte les interactions qui naissent entre les objets, les personnes et les systèmes.

1.4 Dimensions de la sécurité de l'IdO

L'IdO est une technologie caractérisée par une forte ubiquité dans le monde physique et une omniprésence autour de ses usagers. Les diverses applications potentielles de l'IdO, l'hétérogénéité

de ses technologies habilitantes et sa forte dimension humaine et socioéconomique rendent sa sécurité un sujet difficile et complexe. En plus des problèmes de sécurité des technologies qui le constitueront, l'IdO accentue les problèmes de sécurité des personnes qui l'utiliseront, et fait émerger de nouveaux problèmes liés à la sécurité des systèmes sous son contrôle. Comme nous l'illustrons sur la Figure 2, la sécurité et la privacy dans l'IdO peut être abordée à travers trois angles complémentaires qui reflètent ses dimensions technologique, humaine et systémique.

La protection de la technologie concerne en premier lieu la sécurité des données, des communications et des infrastructures réseaux. Cette protection est nécessaire pour contrarier les attaques classiques et futures sur l'intégrité, l'authenticité et la confidentialité des données, ainsi que les attaques sur les infrastructures réseaux et leurs fonctionnalités. La protection des personnes concernera la protection de la vie privée des usagers (« privacy ») qui nécessite, en plus des solutions technologiques, une régulation appropriée qui établit les responsabilités en cas de litiges. La protection des systèmes interconnectés et hébergeant les objets de l'IdO, concernera la protection des objets eux-mêmes livrés à ces systèmes et les processus qu'ils contrôleront.

Figure 2 Sécurité et Privacy de l'Internet des Objets

1.5 Coûts et dommages énormes

Les coûts et dommages engendrés par des attaques véhiculées via IoT sont énormes et proportionnels à la sensibilité des systèmes sous leur contrôle (santé et données personnelles, transport et logistique, énergie et stations nucléaires, finances et commerce électronique, installations industrielles et chaînes de production). De plus, ces attaques et leurs dommages collatéraux ne connaissent pas de frontières géographiques.

Exemple : le vendredi 12 mai 2017, Wana Crypt Or 2.0 un rançongiciel se déploie avec une vitesse fulgurante dans 150 pays. Il infecte en moins de 24h 200.000 victimes sous Windows. Une fois installé sur une victime, il crypte ses données qui deviennent inaccessibles et demande une rançon de 300 USD. Les conséquences de ce malware étaient très sévères : en Grande Bretagne, le système de santé NHS était complètement paralysé, ce qui a provoqué l'annulation d'opérations chirurgicales dont les données des patients étaient devenues inaccessibles ; en France, des chaînes de montage de Renault étaient à l'arrêt avec des pertes financières importantes ; en Allemagne, le transport ferroviaire était perturbé ; aux USA, la chaîne logistique de Fedex était touchée ; en Russie, c'est le système bancaire qui était touché ; en Espagne, Telephonica était atteinte. Etc.

2. Stratégie de cyberdéfense multidimensionnelle

Afin de contrecarrer ces menaces globales l'ITU préconise un agenda de cyberdéfense multidimensionnelle bâtie sur cinq piliers comme illustré sur la figure suivante:

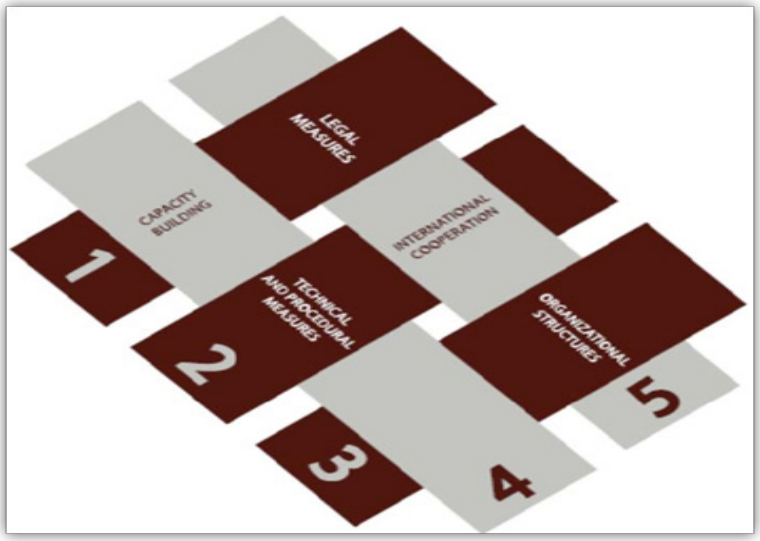

Illustration 4: Agenda de l'ITU de cyberdéfense globale [1]

Dans les sections suivantes, nous présentons un état des lieux des étapes franchies en Algérie dans la mise en œuvre de cette stratégie de cyberdéfense globale et les chantiers qui restent ouverts et requérant toute l'attention des autorités publiques et de la communauté nationale, en vue de bâtir un cyberespace serein et sécurisé.

2.1 Pilier 1 : mesures légales

Sur le plan légal, l'Algérie a franchi des étapes importantes pour organiser l'usage serein des TIC dans le pays, notamment, la loi 09-04 du 5 août 2009 qui définit les règles particulières relatives à la prévention et la lutte contre les infractions liées aux TIC. Afin de bâtir l'infrastructure informationnelle de confiance, la loi 15-04 du 1er février 2015 fixe les règles générales relatives à la signature et à la certification électroniques. Elle a été suivie par la promulgation d'un décret exécutif 16-134/135 le 25 avril 2016 fixant l'organisation, le fonctionnement et les missions des services techniques et administratifs de l'autorité nationale/gouvernementale de certification électronique. Cet organe

étant nécessaire pour l'adoption à large échelle des transactions électroniques et e-commerce en préservant la souveraineté de l'État sur ces types d'échanges et le matériel cryptographique y afférent.

L'IoT est aujourd'hui un véhicule privilégié, de par sa nature omniprésente, pour la collecte d'informations y compris personnelles, pour des fins de marketing (data mining, profilage, etc), recherche médicale et scientifique (enquêtes en amont), et pour des fins d'enquêtes judiciaires et de cyber-renseignement. Cependant, cette collecte à large échelle n'est pas à l'abri de dérives en permettant un accès abusif aux données personnelles et un espionnage massif international. L'avènement de cette nouvelle technologie requiert donc une loi pour la protection des données personnelles instaurant des principes de loyauté envers les usagers, de l'obligation de déclaration de tout système de collecte et traitement de données personnelles aux autorités compétentes, et du déni par défaut de collecte de ces dernières.

Des avancées, dans ce sens, sont attendues très prochainement en Algérie, avec l'adoption par le gouvernement, d'un projet de loi sur la protection des données personnelles lors du conseil des ministres du 27 décembre 2017. A ce titre, le projet de loi énonce notamment l'exclusion des données à usage privé exclusif du traitement en l'objet, la nécessité de l'accord de la personne concernée lors du traitement de ses données personnelles, sauf dans des situations d'obligations légales, essentiellement judiciaires, l'institution d'une protection renforcée pour la protection des données personnelles de l'enfant, et l'institution d'une Autorité nationale de protection des données à caractère personnel, placée auprès du Président de la République.

2.2 Pilier 2 : mesures techniques et procédurales

Ce pilier concerne l'introduction de mesures et procédures globalement acceptables, de schémas d'accréditation et de protocoles et

de standards pour élucider les vulnérabilités dans les produits logiciels et TIC en général. Pour cela, il existe plusieurs normes qui permettent de notifier notamment aux usagers le niveau de sécurité offert par un produit TIC comme les Critères Communs (ISO 15408) ayant pour objectif d'évaluer de façon impartiale, la sécurité des systèmes et des logiciels informatiques.

En Algérie, il est recommandé de contraindre les acteurs TIC à fournir des produits (notamment des systèmes embarqués) avec un niveau minimal de sécurité en exigeant un niveau d'intégration minimal notamment en termes de logiciels et «firmwares» en s'assurant de la fiabilité de ceux-ci.

Vu l'ampleur des produits TIC consommés en Algérie, il est plus que jamais nécessaire de se doter d'un laboratoire national de vérification, de certification et d'homologation de produits TIC importés ou produits en Algérie, car ceci relève de la sécurité nationale.

2.3 Pilier 3 : structures organisationnelles

Ce pilier concerne la mise en place de structures organisationnelles pour la promotion des TIC et leur usage serein et fiable tout en réprimant la fraude et les actes cybercriminels. Dans ce sens, l'Algérie s'est dotée d'un organe national pour la lutte contre les infractions cybercriminelles (Décret présidentiel 15-261 du 8 octobre 2015 fixant la composition, l'organisation et les modalités de fonctionnement de l'organe national de prévention et de lutte contre les infractions liées aux TIC). Parmi les missions qui lui sont assignées on y retrouve :

- la proposition d'éléments de la stratégie nationale de cyberdéfense
- l'animation et la coordination des opérations de cyberdéfense, à savoir :

1. l'assistance des autorités judiciaires et de la police judiciaire en matière de cyberdéfense, y compris à travers le recueil et la fourniture de l'information et des expertises judiciaires ;

2. la surveillance préventive des communications électroniques, en vue de détecter les infractions d'actes terroristes et subversifs et d'atteinte à la sécurité de l'Etat, sous l'autorité du magistrat compétent et à l'exclusion de tout autre organisme national ;

3. la collecte, l'enregistrement et la sauvegarde des données numériques et détermination de la source et la traçabilité en vue de leur utilisation dans les procédures judiciaires.

Néanmoins, le paysage des TIC en Algérie manque toujours d'organes opérationnels pour prévenir et répondre aux attaques cybercriminelles d'une façon efficace et ponctuelle. Il est urgent donc, de se doter d'un CERT (Computer Emergency Response Team) qui permet de réagir promptement à toute attaque ciblant le cyberespace et les infrastructures y afférentes.

2.4 Pilier 4 : renforcement des capacités

Ce pilier concerne l'élaboration des stratégies pour renforcer les connaissances et expertises en cybersécurité. Ça concerne notamment la mise en place d'une stratégie d'immunisation via l'investissement dans le capital humain et en propulsant la cybersécurité dans le calendrier des priorités nationales. Cette stratégie devrait permettre, entre autres, la capitalisation des expertises en cyberattaques et stratégies de cyberdéfense via le CERT. Plusieurs actions doivent être développées en Algérie pour bâtir et renforcer ce pilier et ce, sur plusieurs axes :

- Formation : créer une école nationale de cyberdéfense ayant pour mission de former les experts et officiers spécialistes en cyberdéfense pour répondre aux besoins urgents et évolutifs dans ce domaine.

- Education, vulgarisation et sensibilisation : contraindre les acteurs à informer, sensibiliser les usagers de leurs systèmes d'informations (SI) et produits fournis (notamment les objets connectés et systèmes embarqués) des risques de sécurité. Les différents acteurs doivent coopérer dans la dissémination d'une culture de cyber-hygiène qui permettrait à terme d'estamper beaucoup de défaillance en lien avec un usage inapproprié des TIC.

- R&D en Sécurité Informatique : inscrire cet axe dans les priorités nationales de Recherche et Développement

- Consolidation des capacités de calcul : consolider les capacités nationales en calcul de haute performance pour, notamment, les besoins d'investigations, cryptanalyse, et cyber-renseignement

2.5 Pilier 5 : Coopération internationale

Ce pilier concerne l'élaboration de stratégies pour la coopération internationale, dialogue et coordination. Sur ce plan, l'Algérie est un des acteurs de l'ITU (ONU) qui participe activement à la construction d'infrastructures informationnelles sereines et fiables. L'Algérie participe également au dialogue avec l'OTAN dans le cadre du programme SPS (Science for Peace and Security). Sur le plan de la coopération judiciaire, l'une des missions de l'organe national de lutte contre la cybercriminalité, est de: « veiller à l'exécution des demandes d'entraide émanant de pays étrangers et de développer l'échange d'informations et de coopération au niveau international dans son domaine de compétence ».

Conclusion

Dans cet article, nous avons mis en exergue l'évolution et l'accroissement des attaques et menaces via une forte pénétration d'IoT

accompagnée d'une absence de protection physique d'objets connectés. Ces objets sont pourtant en lien étroit avec les personnes et le contrôle d'infrastructures critiques. L'interconnexion globale de ces objets met donc en danger directement des personnes et des infrastructures critiques, en cas d'attaques cybercriminelles.

Face à cette interconnexion globale et risques multiformes émanant de réseaux de plus en plus globalisés, nous avons montré qu'il est nécessaire de bâtir une stratégie nationale multidimensionnelle de cyberdéfense conformément aux recommandations de l'ITU. Cette stratégie doit être bâtie autour de cinq piliers : mesures légales, structures organisationnelles, mesures procédurales et techniques, renforcement des capacités nationales et la coopération internationale.

L'Algérie a franchi plusieurs étapes importantes vers la mise en place de cette stratégie multidimensionnelle de cyberdéfense. Néanmoins, plusieurs chantiers urgents restent ouverts ou inachevés requérant toute l'attention des autorités publiques et de la communauté nationale pour bâtir un cyberespace et un écosystème TIC serein et fiable en Algérie.

Bibliographie

1. Dr. Frederick Wamala « The ITU National Cyberstrategy Guide » September 2011.
2. Arbia Riahi, Enrico Natalizio, Yacine Challal, Nathalie Mitton, Antonio Iera: A systemic and cognitive approach for IoT security. ICNC 2014: 183-188
3. Arbia Riahi Sfar, Enrico Natalizio, Yacine Challal, Zied Chtourou, « A roadmap for security challenges in the Internet of Things », Digital Communications and Networks, Elsevier, 2017.
4. The Guardian « DDoS attack that disrupted internet was largest of its kind in history, experts say » https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet 2016
5. Sophos Ltd, « Wanna Decrypter 2.0 ransomware attack » https://nakedsecurity.sophos.com/2017/05/12/wanna-decrypter-2-0-ransomware-attack-whatyou-need-to-know/ 2017
6. Maria Garnaeva, Fedor Sinitsyn, Yury Namestnikov, Denis Makrushin, Alexander Liskin, «KASPERSKY SECURITY BULLETIN: OVERALL STATISTICS FOR 2016 », 2016
7. Cloud Security Alliance, "Expanded Top 10 Big Data Security and Privacy Challenges", April 2013.
8. Ovidiu Vermesan et al. "Internet of Things Strategic Research Roadmap", Cluster of European Research Projects on the Internet of Things, 2011.
9. European Research Cluster on the Internet of Things, « Internet of Things : Pan European Research and Innovation Vision", October 2011
10. Y. Law, L. Van Hoesel, J. Doumen, P. Hartel, P. Havinga. Energy-Efficient Link-Layer Jamming Attacks against Three Wireless Sensor Network MAC Protocols. In Proceedings of ACM SASN, Alexandria, Virginia. November 2005.
11. W. Xu, K. Ma, W. Trappe, Y. Zhang. Jamming sensor networks: attack and defense strategies. IEEE.Network. Volume 20, number 3. pp 41-47, May-June 2006.