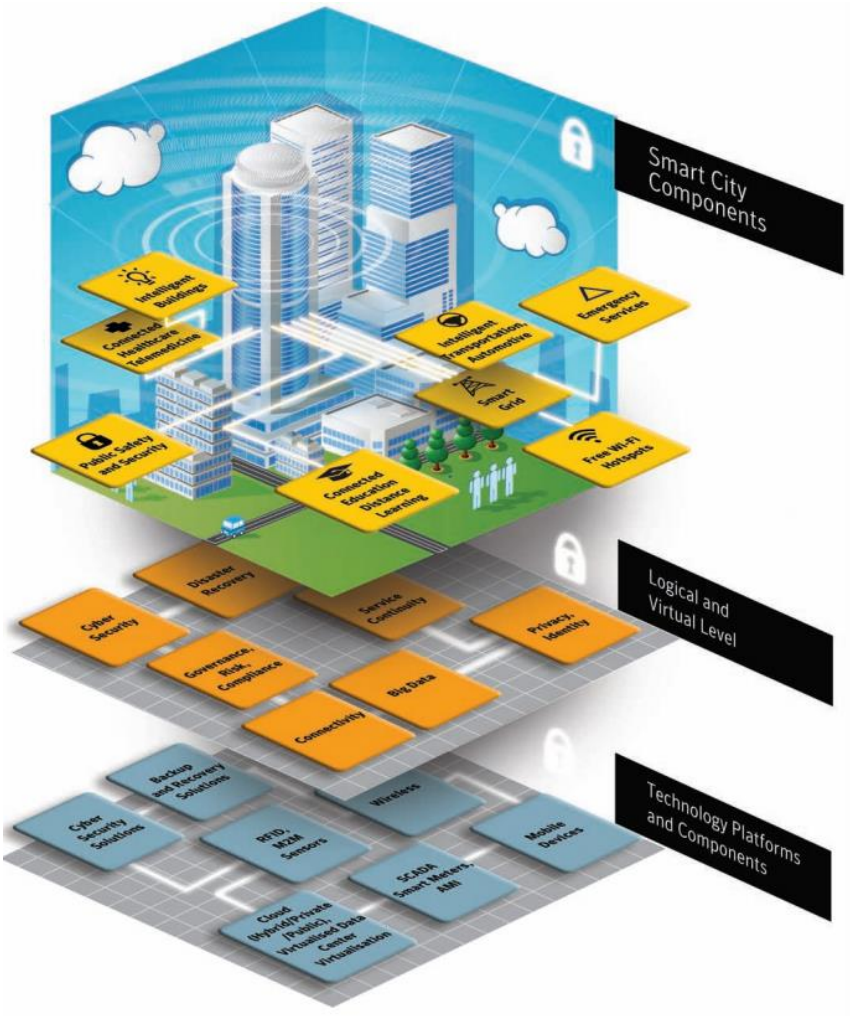
Lettre n°45 - **décembre 2015** - **disponible sur omc.ceis.eu**

«Telecommunications operators and internet service providers shall, according to provisions of law and administrative regulations, put into practice network security systems and information content monitoring systems, technical prevention and safety measures, to avoid the dissemination of information with terrorist or extremist content(…). Network communications, telecommunications, public security, state security and other such departments discovering information with terrorist or extremist content shall promptly order to the relevant units to stop their transmission and delete relevant information, or close relevant websites, and terminate relevant services. Relevant units shall immediately enforce [such orders] save relevant records, and assist in conducting investigations. Departments for network communications shall adopt technical measures to interrupt transmission of information with terrorrist or extremist content that crosses borders online.» ***Article 19 de la nouvelle loi anti-terrorisme adoptée en Chine le 27 décembre 2015***

Table des matières

LES VILLES CONNECTEES : ENTRE RISQUES ET OPPORTUNITES



Source : Symantec

L'émergence des villes connectées

Selon une étude de Gartner publiée en mars 2015[1], le marché des villes connectées, appelées aussi *smart cities*, est en pleine expansion : sur près de 5 milliard d'objets connectés qui sont présents dans le monde depuis la fin d'année 2015, près d'un milliard sont au service de ces villes connectées.

Tous les secteurs sont présents : santé, service public, transports, etc. Les bâtiments et les maisons embarquaient 45% de l'ensemble des équipements connectés fin 2015. Ce chiffre devrait s'élever à 81% en 2020.

[1] http://www.gartner.com/newsroom/id/3008917

Smart City Subcategory	2015	2016	2017
Healthcare	9.7	15.0	23.4
Public Services	97.8	126.4	159.5
Smart Commercial Buildings	206.2	354.6	648.1
Smart Homes	294.2	586.1	1,067.0
Transport	237.2	298.9	371.0
Utilities	252.0	304.9	371.1
Others	10.2	18.4	33.9
Total	**1,107.3**	**1,704.2**	**2,674.0**

Source : Gartner

Une ville connectée est une ville qui cherche à satisfaire des besoins publics via des solutions fondées sur les TIC grâce à l'implication de différentes parties-prenantes : habitants, usagers, collectivités, urbanistes, administrations concernées par l'aménagement du territoire et des villes, et secteur privé (eau, électricité par exemple).

Selon Rudolf Giffinger, qui a théorisé le concept au milieu des années 90, ces villes s'appuient sur 6 piliers, interconnectés, pour devenir intelligentes :

- l'économie intelligente : l'analyse d'une multitude de données en plus de l'accès à de nouvelles sources d'information permettra aux villes de créer des opportunités et de nouveaux emplois ;

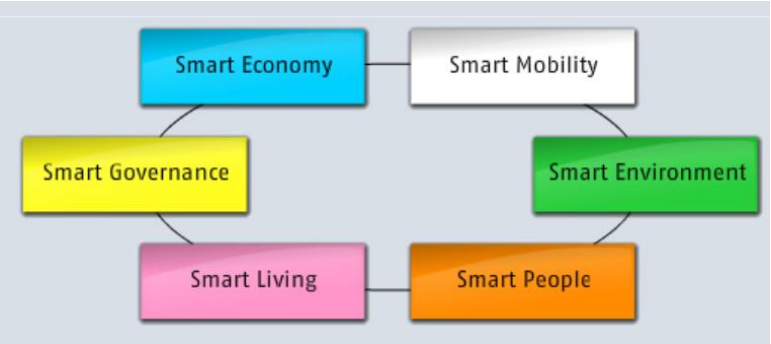
- la mobilité intelligente : l'état de la circulation sur le réseau routier, le temps d'attente aux arrêts et stations de transports en commun, les pannes, etc. Toutes ces informations permettent à l'usager d'améliorer son trajet et à la collectivité d'avoir une meilleure gestion des flux urbains. Cette double action est rendue possible par les divers centres de gestion de données connectés à des capteurs d'informations. Les utilisateurs des transports deviennent en outre eux-mêmes des producteurs de données.

- l'environnement intelligent : la gestion des déchets, de l'eau et de l'énergie sont au cœur des préoccupations des villes en matière d'environnement. En matière d'énergie, les *smart grids* (réseaux de distribution d'électricité intelligents) permettent d'optimiser la production et la distribution d'électricité tout en s'ajustant à la demande en temps réel.

- les citoyens intelligents : l'individu va être l'un des principaux acteurs de la ville connectée. Il doit donc être au cœur du dispositif, à la fois en tant que consommateur et acteur.

- le mode de vie intelligent : les modes de vie des citadins évoluent avec la ville intelligente par la facilitation des déplacements urbains (offres de transports de plus en plus intelligentes et performantes) par exemple.

- la gouvernance intelligente : son objectif est de faciliter la communication, grâce à l'outil informatique, entre les administrations et les citoyens.



Source : Smart-Cities.eu

Il est intéressant de noter qu'aucun de ces 6 piliers ne fait référence à la sécurité alors que chacun d'eux s'appuient sur des informations, avec pour conséquences de nombreux défis en termes de confidentialité (croisement des données des citoyens dans le cadre de leurs interactions avec la ville intelligente), d'intégrité (risques associés à des analyses automatiques erronées en raison de mauvaises données d'entrée) et de disponibilité (équipements connectés accessibles 24h sur 24 et 7 jours sur 7).

Les risques informatiques dans les villes connectées

Le sujet étant nouveau, il n'existe actuellement aucun retour d'expériences sur la manière de protéger une ville connectée.

Il s'agit donc, en premier lieu, d'analyser quel sera le périmètre à protéger au sein de cette ville connectée. Cette démarche permet de relier les enjeux de la ville intelligente aux différentes typologies de SI existants et à leurs vulnérabilités associées.

Un centre de contrôle IT au cœur de la Cité à sanctuariser et redonder

Contrairement aux villes « classiques », les villes intelligentes nécessitent une vigilance supplémentaire : il ne suffit plus de protéger le terrain physique de la ville, mais également son espace numérique. Les centres de commandes de la ville connectée deviennent des endroits très critiques car les données et les commandes informatiques de la ville y sont regroupées dans un même endroit. La probabilité d'occurrence d'une attaque informatique y est donc fortement augmentée, tout comme son impact potentiel.

Les données et la vie des citoyens captées et analysées en permanence

Le caractère symbolique d'une attaque sur une ville connectée est important : la communication autour de l'attaque sera plus forte et pourront susciter nombre de fantasmes qui dépasseront largement la réalité technique de l'attaque. Viendront aussi se greffer des questions de *privacy*, de confiance dans les infrastructures. Il n'est pas difficile d'imaginer la réaction des parents lorsque les caméras des crèches de leurs enfants se retrouveront, à la suite d'une attaque ou d'un défaut de sécurisation, en libre accès sur internet comme cela arrive régulièrement depuis quelques années pour des caméras de particuliers ou d'entreprises.[2]

[2] http://www.zataz.com/un-bot-twitter-diffuse-des-cameras-de-surveillance-non-securisees/

Des risques multiples

Le piratage des panneaux de signalisation, la prise de contrôle de l'éclairage public, ou pire des feux de signalisation peuvent non seulement entrainer une gigantesque pagaille mais aussi générer des risques pour l'intégrité physique des habitants et la sécurité des transports. Ce risque a été démontré par un hacker lillois qui a récemment pris le contrôle des panneaux d'affichage des parkings et a affiché à la place du nombre de places disponibles des propos orduriers. Le même individu aurait également pris le contrôle de l'éclairage public de la ville un an auparavant[3]. Contrairement à la délinquance « classique », face à laquelle les forces de l'ordre peuvent agir directement, la réaction à une attaque informatique sur une ville connectée serait nettement plus complexe, surtout si l'attaque informatique est menée depuis l'étranger. Les municipalités ne peuvent, pour des raisons évidentes de coûts, se doter d'équipes permanentes d'investigation numérique. En cas d'attaque, c'est donc l'échelon national qui devra prendre le relais.

Un empilement critique de solutions logicielles et hardware

Une ville connectée se constitue progressivement de différents éléments, comme des sondes ou des panneaux par exemple, qui sont interconnectés afin de pouvoir remonter, échanger des informations, ou encore être opérés à distance. Ce sont des systèmes IoT peu supervisés, développés par de multiples acteurs répondant à leur propre cahier des charges et sollicités au fil des besoins, la plupart du temps sans vision globale. Il n'y a en outre pas ou peu de mises à jour de sécurité et de moyens de supervision et de détection d'attaques à l'heure actuelle. De plus, leur dissémination au sein de la ville pour une multitude d'usages de niveaux de criticité variés (calcul de l'intervalle entre deux bus *vs* gestion des approvisionnements en eau potable) fait qu'ils sont aujourd'hui peu surveillés et constituent donc autant de *backdoor* physiques permettant potentiellement d'accéder aux serveurs centraux et, ainsi, de prendre le contrôle des infrastructures et des informations de la ville intelligente.

Une gouvernance des données particulièrement complexe

La multiplicité des données nécessaires à la ville connectée implique une gouvernance très complexe. Certaines données doivent être totalement ouvertes (open data), d'autres accessibles pour certaines catégories d'utilisateurs, d'autres encore totalement confidentielles. L'ampleur des systèmes intelligents qui équiperont les villes de demain soulève une autre problématique : alors que les municipalités et leurs infrastructures comptent déjà parmi les systèmes les plus complexes jamais conçus par l'homme, leur superposition avec des processus de collecte et de traitement de données induira forcément de nouveaux bugs et des interactions imprévues. La notion de «réseau interne» n'est en effet plus applicable au sein des villes intelligentes. Selon IO Active[4], la tendance serait : plus la ville est intelligente, plus il existe de systèmes d'information et d'interactions entre les systèmes, et plus l'accès aux données recueillies par tous ces systèmes est ouverte. Il devient donc impossible de faire un réseau « fermé » pour faire communiquer entre tous ces systèmes.

[3] Cela a été le cas pour des panneaux affichant le nombre de places disponibles dans les parkings de Lille : http://france3-regions.francetvinfo.fr/nord-pas-de-calais/lille-des-panneaux-de-parkings-pirates-des-vulgarites-affichees-796843.html

[4] http://www.darkreading.com/vulnerabilities---threats/ioactives-global-call-to-action-smart-cities-must-protect-citizens-from-emerging-cyber-security-threats-/d/d-id/1319825

Des responsabilités encore floues

Enfin, en raison de la jeunesse des villes connectées, la responsabilité légale d'une ville connectée n'est pas encore définie : qui sera le responsable lorsqu'une ville subira une attaque informatique ? Est-ce la ville, l'Etat ou la société ayant vendu, installé voire géré les systèmes d'information ?

Si les vulnérabilités évoquées dans ce document restent relativement classiques en matière de cybersécurité, les villes intelligentes imposent cependant un changement d'échelle dans la prise en compte de ces menaces. Quand le Nord de l'Angleterre est inondé, c'est l'armée qui intervient pour secourir les populations… Si Issy les Moulineaux voit son infrastructure IT compromise, que pourront faire les forces de sécurité ou les forces armées pour garantir l'intégrité de la population et des sièges sociaux des grandes entreprises implantées sur place ?

.

LES NOUVEAUX OUTILS D'ANONYMISATION ET DE COMMUNICATION SECURISEE

De nouveaux moyens de communication (emails, discussions instantanées, VOIP, etc.) ont émergé. Et avec eux des solutions de sécurité qui permettent aujourd'hui de protéger des activités licites mais également illicites. Quels sont les moyens de communication sécurisés existant sur internet ? Quels sont les techniques utilisées par les cybercriminels ou par les organisations terroristes comme Daesh ?

L'anonymat et le chiffrement de données sont en effet l'un des principaux sujets évoqués sur les forums djihadistes. Certaines de ces recommandations concernent les moyens sécurisés utilisables pour transférer des informations sur Internet. D'autres traitent du stockage d'informations chiffrées, aussi bien sur un ordinateur que sur un appareil mobile (smartphone et tablette).

Les outils pour conserver l'anonymat

Dans le monde numérique, de nombreux moyens existent pour conserver son anonymat. Ils peuvent être classés en plusieurs catégories :

<table>
<tr><th colspan="3">Chiffrement de toutes ses activités quand on se connecte à Internet</th></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td colspan="2">FireChat</td><td>The Serval Project</td></tr>
<tr><th colspan="3">Chiffrement des communications par VoIP</th></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>FaceTime</td><td>IO Swisscom</td><td>Linphone</td></tr>
</table>

		
RedPhone	Signal	Silent Circle

Chiffrement et protection des communications instantanées

			
Cryptocat	iMessage	IO SwissCom	PQChat
			
Sicher	SureSpot	Telegram	Threema
			
Wickr			

Chiffrement et protection des fichiers et du matériel

			
Disques durs chiffrés	TrueCrypt 7.1	VeraCrypt	Windows Bitlocker

Hushmail.com	Protonmail.com	Tutanota.com
Navigation de manière sécurisée sur Internet		
Protection quand on publie une photo, à l'aide d'une fausse géolocalisation :		
Mappr		
Protection quand on utilise son téléphone GSM		
Stockage de manière sécurisée		

Copy.com	MEGA
Spideroak	SugarSync

Les formations à l'utilisation de ces outils

Certains outils cités ci-dessus peuvent demander une certaine pratique. Au sein de la communauté djihadistes par exemple, certains membres fournissent de nombreux logiciels, tutoriels et guides pour faciliter l'anonymisation et la confidentialité des échanges.

- Athir Al-Madina, une branche de l'organisation salafiste Ansa al-Charia, a publié une annonce dans laquelle elle fournissait un moyen de la contacter de façon sécurisée, grâce à l'application Telegram, qui envoie des messages chiffrés de bout en bout. L'organisation fournit ainsi un numéro de téléphone dans le message à rajouter pour les contacter sur Telegram.

Source : https://twitter.com/AtherMadina/status/594498449292288000

- Tikni al-Dawla al-Islamiya (*l'homme technologique de l'Etat Islamique*) a publié sur des forums djihadistes de nombreux guides sur la navigation sécurisée, notamment :
    - Une série de cours sur la sécurisation de son ordinateur personnel[5] grâce notamment :

        - A l'installation du système d'exploitation anonyme Tails[6]. Après avoir installé ce dernier, l'utilisateur peut naviguer sur Internet sans laisser de traces. Le système d'exploitation inclut des outils pour chiffrer et protéger la vie privée, ainsi qu'un navigateur internet qui utilise TOR ;
        - A l'installation de l'antivirus Kaspersky[7] ;
        - A l'installation[8] et la navigation avec TOR[9] ;

        - A la protection d'un ordinateur face à un *keylogger*[10] ;
        - Au chiffrement de fichiers avec l'application VeraCrypt[11] ;
        - Au chiffrement d'une clé USB[12] ;
        - A l'installation du VPN de F-Secure[13].
    - Un guide pour créer un compte et utiliser les emails sécurisés sur Hushmail, ProtonMail et Tutanota[14] ;
    - Un ensemble de cours sur la sécurité des téléphones portables[15], incluant :

        - Utilisation des applications Android pour éviter la fuite de données personnelles sur le propriétaire du téléphone[16] ;
        - Indications sur l'utilisation de l'application ORBOT, qui permet de chiffrer le trafic de ses applications Android[17] ;
        - Explications sur le chiffrement d'un téléphone Android ;

---

[5] https://dump.to/windowssec

[6] https://dump.to/TAILS

[7] https://dump.to/Kasper

[8] https://dump.to/Torbrowser

[9] https://dump.to/torformac

[10] https://dump.to/axX

[11] https://dump.to/veracrypt

[12] https://dump.to/USB

[13] https://dump.to/VPN4PC

[14] https://dump.to/Emailencrypted

[15] https://dump.to/ARCHIVE1

[16] https://dump.to/eHY

[17] https://dump.to/Tororbot

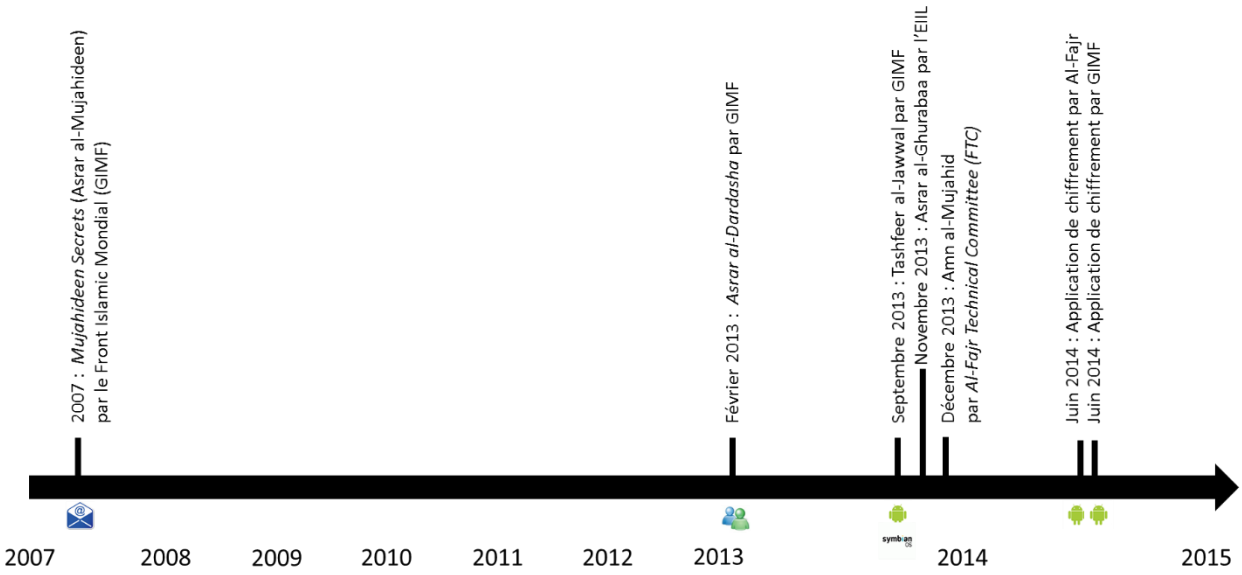
- Précisions sur la façon d'éviter l'utilisation de services comme Google sur Android[18] ;
- Et une dizaine d'autres « cours »…

  - Un guide en anglais sur la manière de protéger l'information sur un smartphone.[19]

- De nombreuses publications sur les techniques pour protéger son ordinateur sont aussi présentes sur les sites de type *Pastit*[20]

- « The Salafi Army of the Nation » de Jérusalem a publié sur Internet un guide pour protéger ses communications. Ce guide avait été réalisé initialement pour des journalistes, présents à Gaza durant l'été 2014, par une société de conseil en sécurité informatique du Koweït, CyberKov[21]. Une quarantaine de produits y sont présentés. Le guide a ensuite été récupéré et une traduction « augmentée » a été réalisée par l'Etat Islamique pour leur communauté.

On observe ainsi que les mêmes méthodes sont utilisées par les djihadistes et les hacktivistes. Seuls les outils peuvent différencier. Par exemple, Amn al-Mujahid (*Securité du Moujahid*) est un outil de chiffrement utilisé principalement par les djihadistes, plus simple que GPG qui est utilisé par les hackers. L'outil existe en version bureau et en version mobile[22] depuis décembre 2013. Suite aux révélations Snowden en juin 2013, les principales organisations djihadistes ont accéléré le déploiement de leurs propres solutions cryptographiques, comme on peut le voir dans la figure ci-dessous.



Evolution des développements des solutions de chiffrements djihadistes – Source : CEIS

[18] http://dump.to/gapps

[19] https://dump.to/protecotionISO2

[20] http://justpaste.it/gyoo

[21] https://cyberkov.com/

[22] http://www.al-fajrtaqni.net/english.html

La **Direction Générale des Relations Internationales et de la Stratégie (DGRIS)** propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation. Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique**, sous le numéro de marché 1502492543. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère de la Défense et des Anciens combattants
Direction Générale des Relations Internationales et de la Stratégie
14 rue Saint-Dominique - 75700 – Paris SP 07

CEIS
280 Boulevard Saint-Germain - 75007 - Paris
Téléphone : 01 45 55 00 20
E-mail : omc@ceis-strat.com