Lettre n°69 - Décembre 2017 - disponible sur omc.ceis.eu

TABLE DES MATIERES

LE RUNET, CONSTRUCTION POLITIQUE OU REALITE TECHNIQUE ?

Si l'internet global peut être perçu comme un espace d'échanges ouvert qui transcende les frontières étatiques traditionnelles, le RuNet suit une approche bien différente, avec notamment une vision politique, sécuritaire, économique et culturelle plus souveraine du cyberespace qui place l'État russe au cœur du développement d'internet.

Le RuNet (contraction de « *Russian internet* ») recouvre des réalités diverses :

- Il est généralement défini comme le segment russophone de l'internet global, ce qui comprend les sites web qui utilisent la langue russe et/ou qui partagent l'histoire et la culture russe. En ce sens, le RuNet est le segment de l'internet global qui réunit toutes les communautés russophones notamment de l'ex-URSS, à la fois au plan culturel et économique ;
- Plus étroitement, il est défini comme l'ensemble des sites web qui ont un nom de domaine russe ou qui sont d'origine russe avec un nom de domaine international « .com » (VKontact.com par exemple) ;
- Enfin, le RuNet est aussi défini comme le segment géographique russe de l'internet global, ce qui fait référence au trafic internet se situant à l'intérieur de la Fédération de Russie.

Initialement, le RuNet s'est développé librement sans intervention forte de l'État fédéral russe. Il a ainsi pu reconstituer l'ensemble de l'écosystème des GAFAM (moteurs de recherche, réseaux sociaux, messageries, e-commerce, etc.)[1]. Le RuNet a alors rapidement gagné en popularité dans les pays de l'ex-URSS. A ce titre, les autorités russes ont peu à peu manifesté leur intérêt pour le RuNet, notamment pour le rayonnement culturel et économique de la Russie. Au cours des dernières années, avec les révélations d'Edward Snowden, les printemps arabes ou encore la révolution ukrainienne, l'Etat russe a renforcé son contrôle et son influence sur le RuNet[2]. Les autorités russes ont notamment adopté une doctrine de cybersécurite en 2016 qui vient préciser les perspectives du RuNet pour les prochaines années à venir.

Quelle est la situation du RuNet aujourd'hui et quelles sont les perspectives envisagées selon la doctrine russe de cybersécurité ?

L'état actuel du RuNet

Actuellement, le RuNet s'articule autour d'un cadre juridique favorable au contrôle de l'internet par l'Etat, d'une infrastructure liée au territoire de la Russie et d'une indépendance technologique vis-à-vis des géants du numérique.

[1] http://en.therunet.com/upload/docs/Runet_Economy_2011.pdf

[2] https://www.numerama.com/politique/286513-ukraine-anatomie-dune-cyberguerre-episode-3-runet-cet-internet-devenu-outil-dinfluence-du-kremlin.html

Le cadre juridique

Depuis 2012, la législation russe n'a cessé de renforcer l'emprise de l'Etat sur le RuNet[3]. Ainsi, la législation permet au *Roskomnadzor*, le service fédéral de supervision des communications, des technologies de l'information et des médias de masse, de prendre des mesures administratives (sans intervention de l'autorité judiciaire) pour censurer les sites web ou contenus en ligne considérés comme portant atteinte à l'ordre public russe. De même, elle permet au gouvernement de contrôler les activités des blogueurs et des médias citoyens dépassant un certain seuil de popularité[4]. Par ailleurs, la législation vise à restreindre l'anonymat sur internet en limitant par exemple les transferts électroniques anonymes de fonds, l'utilisation des VPN et l'anonymat des utilisateurs de messageries comme Telegram[5]. Notons également que la Russie a récemment adopté une loi permettant de qualifier des médias étrangers ou russes d'« agents de l'étranger » lorsqu'ils bénéficient d'un financement international[6].

Enfin, la législation russe dispose que les serveurs et les données relatives au RuNet soient localisées sur le territoire de la Fédération. Cette législation concerne toutes les entreprises numériques qui proposent des services sur le RuNet, ce qui inclut Google, Twitter ou encore Facebook. En outre, il est demandé à tous les opérateurs que les informations et données concernant les utilisateurs du RuNet, qui doivent être stockées sur le territoire de la Fédération, soient conservées pendant une durée minimum de 6 mois.

Si l'inflation législative relative au RuNet a pour ambition d'affirmer la souveraineté de la Russie dans le cyberespace et de protéger ses intérêts, elle suscite toutefois des inquiétudes de la part de la population s'agissant des risques d'atteinte à la liberté d'expression.

L'infrastructure

Actuellement, le RuNet repose sur une architecture qui comprend :

- Des plateformes principalement russes (Yandex, Vkontakte, RuTube, Mail.ru, etc.) dont les serveurs sont hébergés dans des *datacenters* situés sur le territoire de la Fédération ;
- La possibilité pour la Russie, depuis 2010, d'assigner des noms de domaine en .ru, .su et .рф ;
- Des opérateurs privés au niveau national et au niveau local.

Ainsi, il apparaît que le RuNet est un segment géographiquement délimité de l'internet global dont l'architecture dépend encore des opérateurs privés.

A ce titre, soulignons que le gouvernement fédéral a expérimenté, en 2014, une prise de contrôle du RuNet pour l'isoler de l'internet global. Le *Roskomnadzor* avait ainsi ordonné aux opérateurs russes de bloquer le

[3] https://fr.globalvoices.org/2014/07/12/171743/

[4] Les blogueurs et médias citoyens avec plus de 3000 personnes d'audience quotidienne sont tenus de s'enregistrer auprès du gouvernement fédéral

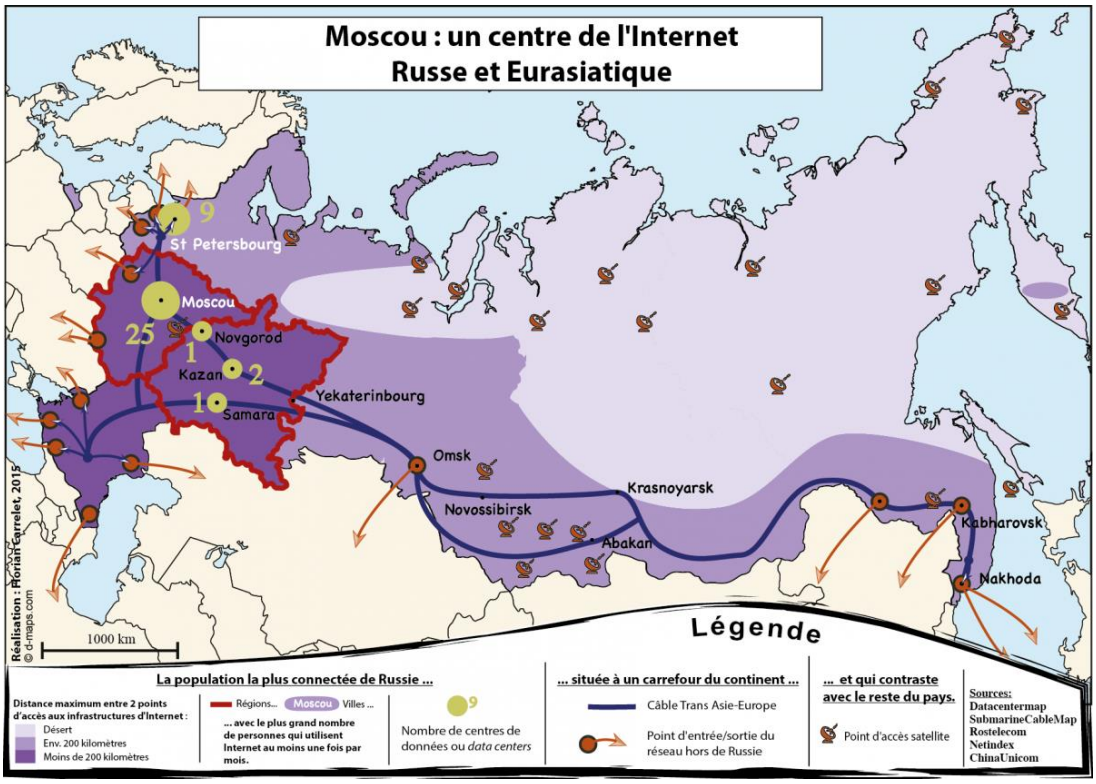
[5] http://www.rfi.fr/europe/20170807-russie-internet-acces-controle-lois-vpn-messageries-anonymat-manifestation-russie-no

[6] http://www.lemonde.fr/international/article/2017/11/15/la-russie-adopte-une-loi-permettant-de-designer-les-medias-comme-des-agents-de-l-etranger_5215092_3210.html

trafic internet en provenance et à destination de l'étranger[7]. Néanmoins, l'opération fut un échec puisque de nombreux opérateurs ont conservé une connexion avec l'internet global.

Notons enfin qu'un projet de centralisation des infrastructures du RuNet au sein de l'organisation russe indépendante MSK-IX a été initié en 2016[8].

Figure 1 : Le RuNet en 2015, un cyberespace géographiquement délimité



(Source : cyberstrategie.org)

L'indépendance technologique

Dans le cadre du développement du RuNet, les autorités russes souhaitent davantage développer leurs propres systèmes d'information afin notamment de ne plus être dépendantes des produits des entreprises américaines telles que Microsoft. Il s'agit donc pour la Russie de développer ses propres capacités numériques.

A ce titre, le ministère de la Défense russe a annoncé en 2016 avoir mis en place pour les besoins de l'armée un réseau baptisé « Segment fermé de transmission de données » (SFTD) qui est entièrement déconnecté

[7] http://www.telegraph.co.uk/news/worldnews/europe/russia/11934411/Russia-tried-to-cut-off-World-Wide-Web.html

[8] http://sevendaynews.com/2016/07/06/take-two-who-will-create-a-backup-of-the-runet/

de l'internet global[9]. Le réseau qui utilise les protocoles de type X.25[10] ne dispose en effet d'aucun accès avec l'internet global.

En outre, la Russie s'est dotée de son propre système de paiement électronique avec une carte bancaire spécifique (Mir) qui est aujourd'hui acceptée en Europe[11]. Il est également prévu que la carte bancaire Mir soit acceptée au sein du système international après 2021.

Enfin, la Russie favorise le développement de processeurs souverains et souhaite également développer un OS alternatif qui servirait notamment pour les terminaux mobiles russes. Un partenariat a été ainsi conclu avec Jolla, l'éditeur de Sailfish, un OS pour appareils mobiles[12], notamment dans le but de ramener à 50% la part des OS Android et iOS qui équipent les terminaux utilisés en Russie d'ici 2025.

Les perspectives du RuNet

Le projet « RuNet 2020 »

Le projet « RuNet 2020 » renvoie à une conception particulière du cyberespace propre à la doctrine russe de sécurité dans « la sphère de l'information »[13]. Selon cette doctrine, le cyberespace s'entend comme un « espace d'information » qui correspond à l'ensemble des activités et moyens traitant de l'information (activités humaines sur internet, infrastructures numériques, contenu de l'information, etc.)[14]. C'est pourquoi la doctrine emploie le terme de « sécurité informationnelle » et non seulement de « cybersécurité ».

A ce titre, la Russie a développé le concept d'une souveraineté numérique qui pourrait se définir comme le droit et la capacité pour un Etat de déterminer lui-même ses intérêts géopolitiques dans le cyberespace. Autrement dit, un Etat pourrait se doter de son propre cyberespace, indépendant de l'internet global et entièrement sous son contrôle. Ce concept trouve une application dans le projet « RuNet 2020 ».

L'un des objectifs de la doctrine russe de « sécurité informationnelle » adoptée en 2016 consiste à acquérir une souveraineté numérique en plaçant le RuNet sous le contrôle de l'Etat fédéral de Russie. Il est ainsi projeté pour 2020 que 99% du trafic internet russe soit situé dans le territoire de l'Etat et qu'il soit également créé 99% des sauvegardes des infrastructures du RuNet sur le territoire.

[9] https://fr.rbth.com/tech/defense/2016/10/19/la-russie-cree-son-propre-reseau-internet-militaire_640393

[10] Protocole de communication utilisant la technique de transfert de données par commutation de paquets en mode point à point. Ce protocole était utilisé pour le minitel en France.

[11] http://blog.economie-numerique.net/2017/06/30/le-lancement-dune-nouvelle-carte-bancaire-mir-sinscrit-dans-un-vaste-programme-visant-a-creer-un-systeme-financier-autonome-en-russie/

[12] http://www.zdnet.fr/actualites/la-russie-veut-faire-reculer-ios-et-android-avec-son-propre-os-39819484.htm

[13] http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163

[14] https://books.google.fr/books?id=uFA8DwAAQBAJ&pg=PA370&lpg=PA370&dq=should+runet+2020

Un outil de défense contre les menaces du cyberespace

Selon la doctrine russe de « sécurité informationnelle », le cyberespace peut constituer une menace tant pour les « valeurs spirituelles et morales traditionnelles russes » [15] que pour les infrastructures numériques russes, notamment avec l'augmentation des cyberattaques.

Ainsi, pour les autorités russes, l'indépendance du RuNet constituerait la meilleure des protections contre les ingérences étrangères et les cyberopérations[16]. En effet, le RuNet constituerait un outil de cyber-dissuasion en rendant plus difficile toute cyberopération contre les infrastructures et réseaux russes.

Notons que dans le cas où le projet « RuNet 2020 » se réaliserait, cette stratégie pourrait avoir pour effet de remettre en question la puissance militaire des Etats disposant d'une grande capacité de cyberopérations.

L'émergence d'un internet indépendant

Dès 2012, les Etats qui forment l'alliance baptisée BRICS (Brésil, Russie, Inde, Chine et Afrique du Sud) ont contesté les monopoles des géants du numérique américain dans la gouvernance de l'internet et ont émis le souhait de réaffirmer leur souveraineté dans le cyberespace[17]. A ce titre, un projet d'internet indépendant avec la construction d'un câble internet reliant l'ensemble des BRICS a été lancé en 2013[18]. Néanmoins, ce projet n'a pas encore été réalisé, semble-t-il, en raison de son coût élevé.

Figure 2 : Les BRICS et le projet d'un câble internet indépendant

(Source : washington.edu)

En revanche, l'idée de créer un internet indépendant de l'internet global demeure présente. En effet, la Russie envisagerait ainsi de doter les BRICS d'une infrastructure internet indépendante pour août 2018[19]. Le projet

[15] https://www.lesechos.fr/06/12/2016/lesechos.fr/0211567177153_la-russie-adopte-une--doctrine--de-cybersecurite.htm

[16] https://www.fiia.fi/sv/publikation/russias-new-information-security-doctrine?read

[17] https://kassataya.com/2013/10/20/internet-enjeu-de-pouvoir-entre-les-etats-unis-et-les-grands-emergents/

[18] https://jsis.washington.edu/news/reactions-u-s-cybersecurity-policy-bric-undersea-cable/

[19] https://www.developpez.com/actu/176798/La-Russie-travaille-a-la-mise-sur-pied-d-une-infrastructure-DNS-a-l-usage-des-BRICS-regards-braques-sur-aout-2018/

consisterait à créer une alternative au système de noms de domaine (DNS). Ainsi, dans le cas où ce projet serait mené à son terme, le RuNet devrait logiquement rejoindre cette nouvelle infrastructure indépendante de l'internet global. Reste à connaître les modalités et donc les conséquences de l'adhésion à cette nouvelle infrastructure au regard de l'internet global.

LES RESEAUX AD HOC MOBILES : RISQUES ET OPPORTUNITÉS

Fonctionnement

Qu'est-ce qu'un réseau ad hoc?

Un réseau ad hoc (ou réseau IBSS, *Independant Basic Service Set*) est un réseau autonome, sans fil, auto-configurable, déployable rapidement et en tous lieux, permettant de communiquer sans s'adosser à une infrastructure existante. Il se passe de point d'accès : chaque appareil est à la fois émetteur et récepteur. Il peut notamment sous forme d'un réseau de smartphone (*Mobile Ad hoc NETworks, MANET*) à l'aide d'une application dédiée.

Selon la définition du groupe de travail IETF[20], un tel réseau « comprend des plates formes mobiles (par exemple routeurs interconnectant différents hôtes et équipements sans fil) appelées nœuds qui sont libres de se déplacer sans contrainte. Un réseau ad-hoc est donc un système autonome de nœuds mobiles. Ce système peut fonctionner d'une manière isolée ou s'interfacer à des réseaux fixes au travers de passerelles. Dans ce dernier cas, un réseau ad-hoc est un réseau d'extrémité[21] ».

Cette technologie a l'avantage de pouvoir être mise en œuvre dans les zones aux infrastructures de télécommunication inopérantes puisqu'elle permet d'établir, dans de brefs délais, un réseau efficace, peu exigeant en ressources.

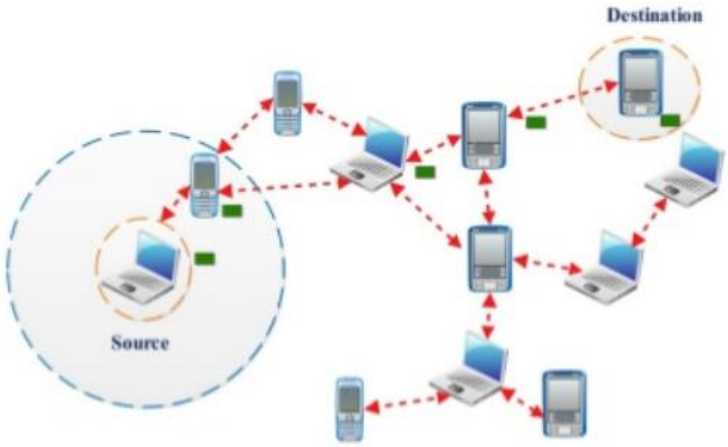


Figure 1: architecture de connexion ad-hoc
(Source: https://www.slideshare.net/bentchebbah92/simulation-dun-rseau-adhoc-sous-ns2)

[20] Internet Engineering Task Force

[21] http://www.pouf.org/documentation/securite/html/node27.html

Fonctionnement

L'intérêt d'un réseau ad hoc réside dans le fait qu'il n'y a plus de différence entre un routeur et un récepteur. A l'identique d'un réseau informatique doté de routeurs, une entité (ici, un *smartphone*) peut communiquer sans forcément être à la portée de la station destinatrice, le routage des données transitant par un ou plusieurs *GSM*.

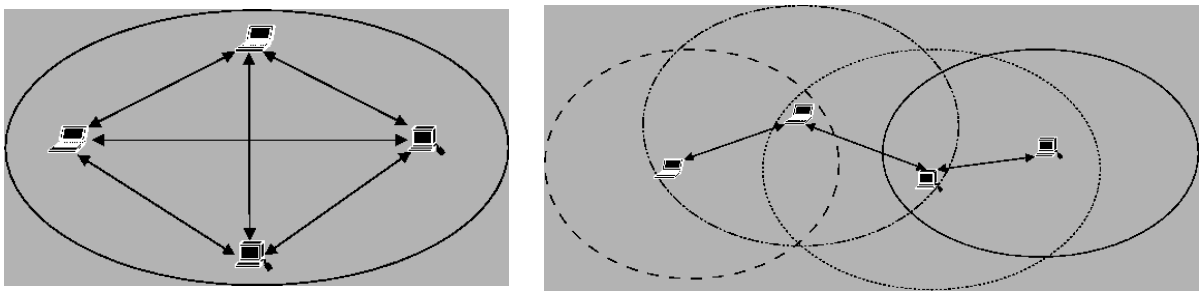


Figure 2: topologie d'un réseau ad-hoc monosaut et d'un réseau ad hoc multisauts

Concrètement, l'appareil transmet la voix et les messages type SMS soit par *Bluetooth*, si le récepteur est suffisamment proche, soit en WI-FI, à travers les points d'accès sans fil d'un réseau IP.

Dans le cas d'un réseau IP existant, un protocole de routage (actif, proactif ou hybride) permet de rediriger les données vers le ou les appareil(s) destinataire(s).

La particularité de ce type de réseau est que les stations et donc les routeurs sont mobiles[22], ce qui n'est pas le cas dans un réseau informatique. Si les routeurs se déplacent, les nœuds aussi. Cela impose des mises à jour des tables de routage rendues possible par des algorithmes spécifiques. Ainsi, si une route établie passe par l'intermédiaire d'une station devenue inaccessible, l'algorithme permet de trouver une autre route pour atteindre le destinataire. C'est la raison pour laquelle on retrouve deux grandes familles d'algorithmes / protocoles : ceux de routage proactif et ceux dits actifs.

Les protocoles de routage proactif se basent sur le même principe que ceux employés dans les réseaux filaires. Ils utilisent des méthodes de vecteur de distance et d'état de lien, chaque entité se renseignant de son environnement et de l'état du trafic en envoyant des messages « hello ». On retrouve les protocoles OLSR (*Optimized Link State Routing*), DSDV (*Dynamic Destination-Sequenced Distance-Vector*)[23]. L'objectif de ces algorithmes est de **maintenir le réseau**.

Les protocoles de routage actifs sont plus spécifiques aux réseaux mobiles puisqu'ils créent des routes « **à la demande** ». On retrouve des algorithmes type DSR (*Dynamic Source Routing*) ou AODV (*Ad-hoc On-Demand Distance Vector*) voire RDMAR. Contrairement aux proactifs, ces protocoles vont essayer de « découvrir » la route vers le destinataire uniquement lorsque la station cherche à communiquer avec lui sans construire une

[22] Une station mobile peut se trouver à un instant t à la portée d'une station et ne plus l'être à l'instant t+1.

[23] On peut aussi noter : FSR, DREAM, Babel, …

table de routage qui lui permettrait de joindre l'ensemble des stations du réseau (ce qui pourrait être lourd sur le plan logique, notamment si les mobiles se déplacent).

On trouve d'autres familles de protocoles moins utilisés :

- ceux dits **hybrides**, alliant les capacités proactives en local et réactives en extérieur (tels que ZRP et ToRA);
- ceux dits **hiérarchiques**, basés sur une structure spécifique autour d'entités élues pour des rôles particuliers : HSR, VSR ou CBRD.
- enfin existent les protocoles dits **géographiques**, basés sur l'utilisation d'informations sur la position des nœuds mobiles (tels que LAR, GRID ou ZHLS)[24].

Chaque type de protocole possède ses avantages et ses inconvénients[25]. Les protocoles proactifs, par exemple, favorisent le délai de routage mais sont lourds à maintenir à jour. A l'opposé, les actifs permettent de maintenir seulement les routes utilisées mais perdent en temps de routage car ils doivent découvrir la route spécifique à chaque destinataire. Il s'agit de savoir ce qu'on recherche et de trouver le bon équilibre (qui peut être défini dans un protocole hybride).

Un protocole dit réactif permettra un meilleur passage à l'échelle, réduisant de manière significative la charge de trafic dans le réseau et ce grâce à la non-diffusion périodique des informations de topologie. Il sera par ailleurs mieux adapté aux réseaux mobiles disposant d'une bande-passante limitée.

Une approche proactive offrira, elle, un meilleur temps de latence pour établir une route. Un tel protocole ne nécessitera pas de mécanisme préalable de découverte.

Un protocole hybride offrira un compromis entre la charge de trafic et le temps de latence.

Cas d'usage et perspectives

Les cas d'usages actuels

Une application classique, vise à permettre de communiquer entre unités de secours sur des zones larges, notamment en cas de catastrophes naturelles. Ce fut par exemple le cas, en Floride, lors de l'approche de l'ouragan Irma où un tel réseau fut déployé pour permettre aux habitants de continuer à communiquer en dépit des infrastructures saturées, puis détériorées après le passage de l'ouragan. L'application Zello, ne nécessitant qu'une connexion Internet et transformant les mobiles en talkie-walkie, fut ainsi mise à profit dans le cadre d'un réseau d'entraide.

Une telle technologie peut aussi être employée pour contourner la censure comme ce fut le cas en Turquie en 2013, au Venezuela en 2014 lors du mouvement de protestation contre le président Maduro ou encore à Hong-

[24] http://fr.calameo.com/read/0000007229c7146e6c4c4. Le lien donne un descriptif détaillé de l'ensemble des protocoles cités. Un autre lien utile : http://slideplayer.fr/slide/5391499/

[25] https://www.slideshare.net/bentchebbah92/simulation-dun-rseau-adhoc-sous-ns2

Kong la même année, qui popularisa l'application *FireChat*[26]. Cette dernière utilise l'émetteur Bluetooth ou le système Wifi des mobiles pour établir des communications directes entre appareils. Les smartphones, situés à quelques dizaines de mètres les uns des autres, se reconnaissent et créent un réseau local temporaire autonome, en *peer-to-peer* intégral.

Perspectives

Les réseaux ad hocs laissent entrevoir de nombreuses perspectives

- Palier les zones blanches

Lorsque surviennent des évènements majeurs susceptibles de détruire / détériorer les infrastructures nécessaires aux télécommunications, de nombreuses zones grises voire blanches se créent. Le déploiement de réseaux *ad hoc* peut être une solution temporaire en attendant le total rétablissement. A noter qu'un des aspects les plus prometteurs dans ce type de réseaux de maillage est sa capacité à se « ré-assembler » pour s'adapter aux modifications de son environnement. La société *MeshNetworks* travaille d'ailleurs sur de tels réseaux mobiles et flexibles pour la sécurité publique. « Des équipages de pompiers dans une scène de catastrophe formeront un réseau sans fil *ad hoc* où tous les périphériques se verront les uns les autres », selon Peter Stanforth, directeur technique de *MeshNetworks*. Parallèlement, la société travaille sur le déploiement de réseaux à large bande qui offriront aux villes l'opportunité d'améliorer l'efficacité et la qualité de services communautaires notamment dans le cadre de travaux publics ou de mesures sécuritaires.

- Transport intelligent, télématique

Dans la même logique que les voitures connectées, le réseau de maillage mobile pourra mailler les autoroutes, chaque véhicule devenant alors un nœud de routage. Moteran (*Mobile Telecommunications radio and Relay Networks*) est un partenariat entre Mitsubishi et Deutsche Telekom qui est équipé de voitures, dans certaines villes allemandes, dotées d'équipement de réseau à large bande pour le divertissement et les communications. Le partenariat prévoit de développer une application permettant d'alerter les conducteurs en cas d'embouteillages, d'accidents, de situations d'urgence ou de toutes informations susceptibles de fluidifier le trajet.

- Maison numérique, domotique

La tendance actuelle est au développement de réseaux sans fil au sein des habitations, le but étant de profiter de plus en plus des facilités offertes par le numérique (distribution multimédia intégrée, aide à l'habitant, surveillance, …). Ces réseaux deviendront de plus en plus complexes, hébergeront de plus en plus de contenus, offriront des résolutions de plus en plus élevées sur de multiples appareils reliés les uns aux autres. Il sera alors nécessaire de trouver un compromis entre bande passante et gamme / couverture.

- Du e-commerce au m-commerce

Le m-commerce (*mobile-commerce*) met en rapport direct les vendeurs et acheteurs (exemple : vente/ achat de billets d'avion/ train de dernière minute dans un aéroport/ une gare), au gré d'un réseau au sein duquel

[26] Si ce n'est pour être téléchargée.

chaque entité fera office de nœud de routage. On retrouve dans le concept la notion de mobilité et de dynamisme de tels réseaux.

Une autre application envisageable permet le déploiement de réseaux militaires qui pourraient être utilisés afin d'assurer la liaison permanente entre les différentes unités (notamment avec le développement de réseaux d'objets connectés).

Les limites des réseaux ad hoc

Aussi utiles puissent-ils être, l'absence d'infrastructures qui caractérise les réseaux ad-hoc fait malgré tout apparaître de nouveaux problèmes :

- En termes de **performances** du réseau : outre les limites en bande passante, la mobilité des dispositifs entraîne des pertes de routage et des erreurs de transmissions qui amènent à des pertes de données. L'hétérogénéité des nœuds, notamment en termes de capacités de traitement (calculs, mémoires) exacerbe ce problème et nécessite une adaptation dynamique des protocoles de routage ;
- En termes **d'efficacité énergétique** et donc d'autonomie des dispositifs. Une grande partie de l'énergie disponible est consommée par la fonction routage du réseau ad hoc ;
- En termes de **sécurité**. Les possibilités de le pénétrer sont plus grandes, la détection d'une intrusion ou d'un déni de service plus délicate. Les réseaux ad hoc sont en outre particulièrement vulnérables aux interférences.

Conclusion

Il est aujourd'hui relativement aisé de créer des réseaux de communication « ad hoc » à moindre frais échappant aux relais GSM traditionnels, premiers vecteurs de géolocalisation et d'interception des communications.

Ces nouvelles « opportunités » de communication peuvent représenter :

- Un atout : s'affranchir de relais fabriqués par des puissances étrangères qui pourraient les rendre inopérants du jour au lendemain.
- Un risque : voire émerger des « sous-réseaux » échappant à tout contrôle et utilisant ces applications pour planifier des attaques terroristes – comme c'est le cas aujourd'hui avec l'application de messagerie Telegram dont la médiatisation devrait logiquement entraîner l'abandon – voire synchroniser des actions en parallèle.

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
Direction Générale des Relations Internationales et de la Stratégie
60 Boulevard du Général Martial Valin – CS21623 – 75 509 Paris Cedex 15

CEIS
Tour Montparnasse – 33, avenue du Maine – BP 36 – 75 755 - Paris Cedex 15
Téléphone : 01 45 55 00 20
E-mail : omc@ceis.eu