Rapport sur le nomadisme numérique

à l'IN2P3

décembre 2009

Serge Bordères (coordinateur) – CENBG
Gérard Drevon – Centre de calcul
Sylviane Molinet, - IPHC
Sébastien Geiger - IPHC
Thierry Mouthuy – CPPM
Jérôme Pinot – SUBATECH
David Zwolinski - LPC-Caen

1 Introduction

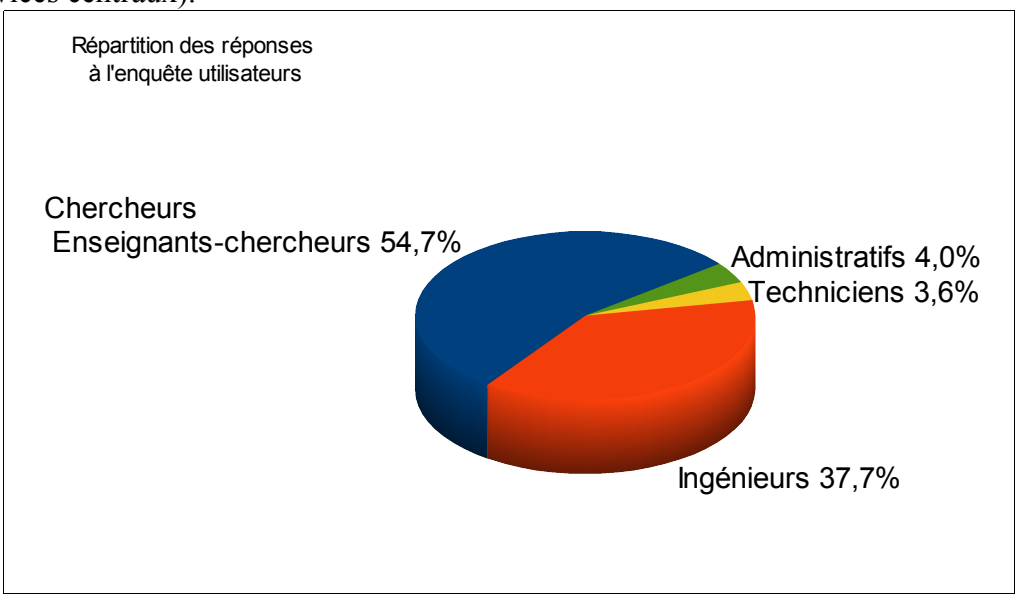
Le présent rapport fait suite à une demande du CCRI (Conseil de Coordination du Réseau des Informaticiens de l'IN2P3) pour une étude prospective du nomadisme dans l'institut. Il a été élaboré par un groupe de travail qui a notamment utilisé les résultats de deux enquêtes. Une était à destination de l'ensemble des personnels de l'IN2P3 en leur qualité d'utilisateur, l'autre à destination des services informatique des unités.

Le résultat de l'étude se décompose en trois documents :

- Le présent rapport qui analyse les problématiques soulevées par le développement du nomadisme d'une façon générale et plus particulièrement replacé dans le contexte de l'IN2P3 grâce notamment aux réponses aux enquêtes. Les chapitres 1 à 6 font un état des lieux et expriment un certain nombre de propositions. Le chapitre 7 reprend ces propositions en les synthétisant et met en avant les points cruciaux sur lesquels il sera important de travailler spécifiquement.
- L'annexe A qui est le résultat brut de l'enquête utilisateurs. On y trouve notamment les commentaires exprimés par les utilisateurs.
- L'annexe B qui est le résultat brut de l'enquête vers les services informatique.

1.1 L'enquête utilisateurs

L'enquête à destination des utilisateurs était composée de 20 questions et avait pour objectif de recueillir les usages et la perception des personnes par rapport au nomadisme. Elle a été envoyée à 2950 personnes (permanents et non-permanents) à partir de l'annuaire (LDAP) de l'IN2P3. Elle a recueilli 442 réponses, soit une participation brute de 15%. Cependant, il était clair que tous les personnels ne sont pas concernés par le nomadisme ou, en tout cas, pas au même degré. Le graphique de répartition des réponses par statut montre bien que les chercheurs (y compris enseignants-chercheurs et doctorants) et ingénieurs représentent en nombre la population la plus concernée (92% des réponses). Les réponses émanent de 23 unités (18 laboratoires, CC, GANIL, LSM, services centraux).



1.2 L'enquête vers les services informatique

L'enquête à destination des services informatique a été soumise à 21 unités (18 laboratoires, CC, GANIL, LSM). Seize ont effectivement répondu.

Cette enquête avait pour but de recueillir des informations plus techniques sur les solutions mises en œuvre dans chaque unité. Elle comprenait 63 questions.

2 Problématique générale et définition

Le développement des ordinateurs portables, l'accroissement de la puissance d'Internet, le développement des technologies de réseau sans-fil, la convergence avec les technologies de téléphonie et leur disponibilité de plus en plus grande aussi bien dans des lieux publics, privés ou professionnels, ont mis à la disposition de chacun de nous des outils puissants que nous nous sommes vite appropriés parce qu'ils nous procurent un potentiel énorme qui a naturellement rencontré une caractéristique majeure de notre activité de recherche : la mobilité. Les agents des unités de l'IN2P3 (et plus généralement de la recherche) ont un territoire professionnel qui ne se limite pas à leur unité propre. Les technologies facilitant la continuité de leur activité professionnelle et la capacité de garder un cordon ombilical avec leur base pour disposer de toutes leurs ressources, de partout et à tout moment, rencontrent naturellement un grand succès. L'ordinateur portable est devenu un bureau mobile.

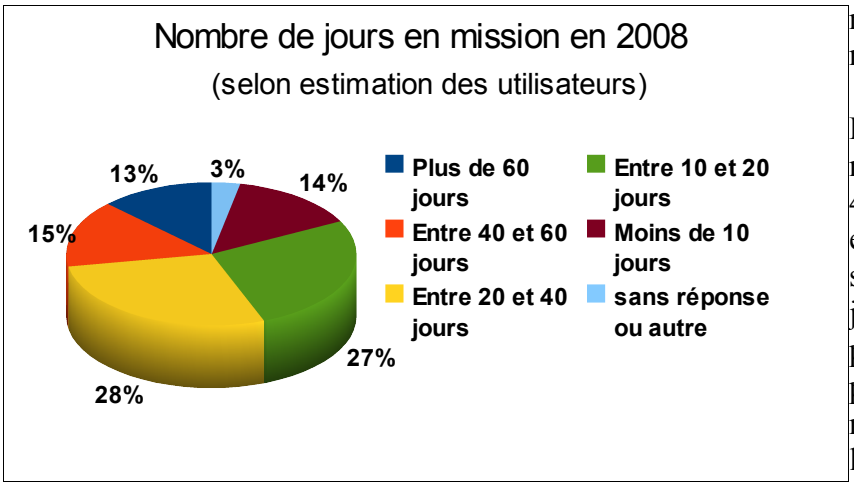
Cette situation entraîne des bouleversements qui ne peuvent pas être sans conséquence sur nos organisations informatiques. De nouveaux problèmes et de nouveaux risques sont apparus, qui ont compromis les repères habituels. Il est désormais important de susciter une véritable politique du nomadisme apte à favoriser de façon responsable le développement et l'usage des technologies liées au nomadisme. L'objectif de ce rapport est de faire une étude de la situation perceptible aujourd'hui mais pas d'en faire une analyse de risques exhaustive.

Définition

On peut considérer que l'on se trouve en situation de nomadisme dès lors que des ressources informatiques professionnelles (matériels, logiciels, données) sortent du périmètre central du système d'information d'une unité ou bien sont utilisées depuis l'extérieur de ce périmètre de façon autonome ou connectée. C'est à partir de cette définition que sera faite l'analyse du présent rapport.

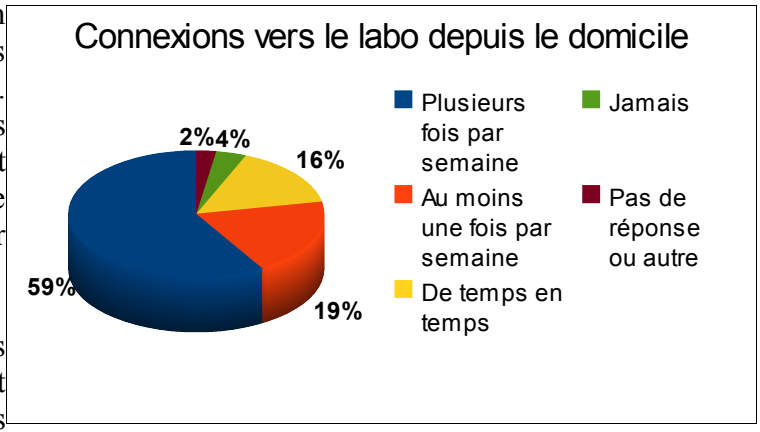
3 Usages du nomadisme

Il est difficile de quantifier précisément l'utilisation du nomadisme dans notre institut. Cependant on peut en avoir une idée générale en observant deux paramètres.
D'une part, en regardant le nombre de jours qu'un agent passe en mission. Plus il est en mission, plus il sera demandeur de moyens nomades. L'enquête demandait aux personnes d'estimer le nombre de jours qu'ils ont passé en mission en 2008.



Plus du quart déclare avoir été en mission plus de 60 jours ou entre 40 et 60 jours et un autre quart entre 20 et 40 jours. Ce qui signifie, si on considère que 20 jours correspondent à un mois professionnel, que la moitié des personnes sont en mission, au moins, entre 1 et 3 mois dans l'année. Ce résultat ne tenant pas compte des déplacements locaux, non comptabilisés comme des missions, mais nécessitant aussi l'usage de ressources informatiques.

Le temps passé en mission n'est pas le seul indicateur de l'usage du nomadisme. L'autre paramètre qui peut être considéré est le travail à distance, depuis le domicile. On peut en avoir une idée au travers des réponses à la question portant sur les fréquences de connexions vers le laboratoire depuis le domicile. 59 % répondent se connecter plusieurs fois par semaine (et certains précisent tous les jours). 19 % déclarent se connecter au moins une fois par semaine.



Ces paramètres montrent bien que les facteurs poussant au nomadisme sont bien présents dans notre institut et qu'ils sont loin d'être négligeables. D'ailleurs 84% des personnes ont estimé que l'usage de ressources informatiques internes depuis l'extérieur est essentiel ou important pour leur activité.

Si le temps passé en situation nomade est un facteur important, le type d'usage qui en est fait est aussi significatif. Il y a quelques années, l'usage à distance correspondait essentiellement à l'accès à la messagerie. Même si ce service reste prépondérant, l'éventail de fonctionnalités devenues utiles, voire indispensables, à distance s'est considérablement accru et rejoint de plus en plus les fonctionnalités disponibles en interne. Par exemple, l'accès aux fichiers centraux, à des machines ou applications internes. Mais aussi l'accès aux bases de données bibliographiques ou l'utilisation de licences normalement accessibles uniquement depuis l'intérieur de l'unité.

Il existe aussi des activités distantes très spécifiques à notre domaine de recherche : la surveillance à

distance d'expériences. Cette possibilité rend d'énormes services aux utilisateurs puisqu'elle leur permet de garder un œil sur leurs expériences qui fonctionnent 24 heures sur 24, 7j/7 avec un minimum de contraintes, depuis chez eux ou lorsqu'ils sont en déplacement. Environ 38% déclarent utiliser cette possibilité (de quotidiennement à parfois).

A l'inverse, on constate aussi le phénomène « d'expérience mobile ». C'est-à-dire une équipe entière part avec ses moyens propres vers un site externe pour utiliser un grand instrument scientifique. C'est un véritable petit réseau qui se déplace ainsi avec des machines d'acquisition et un ensemble de portables. Le cordon ombilical est là aussi un avantage incontestable puisqu'il permet à ces équipes de garder une liaison avec leurs ressources restées sur leur base ou encore de rapatrier directement leur données sans passer par des supports intermédiaires. En somme, travailler sur le site d'expérience et continuer à travailler comme s'ils étaient dans leur bureau.

4 Le mélange des sphères

Les technologies nomades et leur appropriation par les utilisateurs ont développé de nouveaux comportements qui contribuent à accentuer le mélange des diverses sphères dans lesquelles chacun évolue. Par le biais de l'informatique, l'activité professionnelle se trouve désormais de plus en plus en interaction, voire en concurrence, avec des moyens appartenant aux usagers, des moyens appartenant à des tiers, souvent peu identifiables, ou encore des offres commerciales grand public. Celles-ci, bien qu'en général gratuites, n'en sont pas moins des offres du secteur commercial. Dans la suite du document nous utiliserons le terme « opérateurs commerciaux » pour qualifier les sociétés à l'origine de ces offres.

4.1 Interactions avec la sphère privée

Du fait de la disponibilité de liaisons haut-débit à domicile et de la démocratisation des ordinateurs on constate de plus en plus d'interactions entre les moyens privés des personnes et leur environnement professionnel. Nous utiliserons le terme « privé » plutôt que « personnel » pour désigner les moyens dont les personnes sont propriétaires. Le terme « personnel » étant souvent utilisé dans la conversation courante pour désigner l'ordinateur professionnel mis à disposition. Ceci démontrant déjà en soi l'amalgame qui peut être fait.

Un tiers des utilisateurs déclarent utiliser un ordinateur privé dans le cadre professionnel.
Cette situation a plusieurs origines exprimées par les utilisateurs :

- L'utilisateur n'a pas d'ordinateur portable professionnel.
- Le portable professionnel est dépassé par rapport à l'ordinateur privé (fixe ou portable) soit en terme de puissance soit d'un point de vue technologique (poids, capacité des batteries...)
- Même quand on dispose d'un portable professionnel, pour ne pas devoir systématiquement le transporter entre bureau et domicile, il est plus pratique d'utiliser un ordinateur privé.
- La possibilité d'utiliser son poste privé pour réduire les contraintes d'interaction entre vie privée et professionnelle (par exemple nécessité de surveiller une expérience le week-end).

Cette situation a quelque chose d'assez logique. Si on se place du point de vue de l'utilisateur, il se trouve à la tête d'un mini-système d'information dans lequel il doit composer avec ses moyens privés et des moyens professionnels et il tend donc naturellement à se simplifier sa « gestion » informatique. Pour faire une comparaison, c'est comme si on fournissait à chacun une voiture de

fonction pour faire le trajet domicile-bureau. Mais il serait interdit, sur le chemin du retour, de faire un crochet pour aller faire les courses par exemple. Donc au final ce serait une perte de temps car il faudrait retourner chercher sa voiture personnelle et, en plus, disposer d'une place de parking supplémentaire. Et finalement on préfèrerait utiliser sa voiture personnelle. C'est un peu la même situation que l'on retrouve avec les ordinateurs.

Le mélange des sphères ne se fait pas que dans un sens. Si on constate l'utilisation de moyens privés dans l'activité professionnelle, l'inverse existe aussi. C'est-à-dire des moyens professionnels aussi utilisés pour des activités privées. En effet, de plus en plus souvent les utilisateurs (70%) disposent des privilèges administrateurs sur leur poste professionnel. Ils ont donc la possibilité d'installer des logiciels qui sortent du cadre professionnel.

Cependant, ce qui paraît pratique à l'utilisateur a priori peut finalement lui compliquer sérieusement la tâche puisqu'il finit par se retrouver seul pour gérer son informatique car les services informatiques des unités ne produisent pas de supports pour les moyens privés. De plus, des systèmes d'exploitation et des logiciels mal gérés peuvent augmenter le risque de propagation virale vers le milieu professionnel.

Une première approche pourrait consister à interdire l'usage de postes privés dans l'activité professionnelle que ce soit à l'intérieur de nos unités ou à distance. Même si on disposait de moyens techniques complètement fiables pour atteindre un tel objectif, il n'est pas sûr que le résultat ne serait pas contre-productif en favorisant ainsi des situations « clandestines » bien plus risquées et sans aucune visibilité. D'ailleurs, des agents de toutes les unités déclarent utiliser un poste personnel dans leur activité professionnelle, même ceux qui appartiennent à des unités qui ne les autorisent pas sur leur réseau interne... (les politiques dans ce domaine vont de l'interdiction à l'ouverture totale en passant par des sous-réseaux spécifiques ou un traitement de type « visiteurs »).

Les innovations technologiques qui ont contribué à l'usage de matériels privés n'ont pas de raison de s'arrêter et un principe d'interdiction pur et simple risque bien d'être balayé. Par exemple, l'usage des PDA (Personnal Digital Assistant) ou des Smartphones se développe (11% déclarent déjà en utiliser) et il s'agit d'un matériel utile aussi bien professionnellement que dans la vie privée. Les PDA et autres smartphones sont en fait de véritables petits PC qui peuvent se connecter aux réseaux et qui mêlent informatique et téléphonie. Leur évolution et leur aspect pratique ne manqueront pas d'apporter des questions. Chaque utilisateur devra-t-il posséder deux PDA, un privé et un professionnel ? Va-t-on enrayer leur utilisation sous le prétexte qu'ils contribueront au mélange des sphères alors qu'il serait au contraire bon de contribuer à leur usage dans certains cas ? (voir le paragraphe 4.4 « Démêler les mélanges »). Il est probable que les évolutions technologiques, accentuées par les habitudes de type télétravail, vont sans arrêt remettre en question la limite entre les sphères privées et professionnelles.

4.2 Interaction avec le domaine commercial

Depuis que les particuliers ont un accès facile, rapide et permanent à l'Internet, les opérateurs commerciaux n'ont cessé de leur fournir des applications gratuites de plus en plus innovantes et qui finissent par s'avérer aussi utiles en milieu professionnel.

Déjà depuis quelques années existent des applications de messagerie mises en ligne, soit par les fournisseurs d'accès ADSL, soit par d'autres sociétés indépendantes telles que Google ou encore Yahoo. Depuis longtemps, on sait que des personnels du monde de la recherche ont domicilié leur courrier sur ces serveurs indépendants plutôt que dans leur laboratoire ou organisme de rattachement.

Les raisons sont multiples : impossibilité ou difficultés d'accéder au service de messagerie de l'unité, interfaces utilisateur plus pratiques, volonté de centraliser courrier personnel et professionnel, volonté de conserver la même adresse électronique en cas de changement d'affectation, capacité de stockage importante.

18% des personnes ont déclaré dans l'enquête utiliser professionnellement un service de messagerie autre que celui fourni par leur unité ou plus généralement par l'IN2P3. Dans ce chiffre, il y a des cas spécifiques (utilisation de la messagerie d'un autre organisme de rattachement) mais la plupart mentionnent qu'ils utilisent ou qu'il leur arrive d'utiliser des messageries « commerciales » souvent pour des raisons de facilité d'accès de partout, mais aussi souvent parce que le service Webmail (Horde) de l'IN2P3 est considéré comme peu convivial et plus généralement dépassé.

Les services mis à disposition dans le cadre professionnel sont en complète concurrence avec les offres commerciales. Et le paysage est en cours d'évolution car les opérateurs commerciaux proposent de plus en plus de services comme des agendas, des planifieurs, des espaces de stockage, des logiciels de traitement de textes, des sites web personnels, des blogs.

Cette situation présente un certain nombre de problèmes. Tout d'abord des problèmes de sécurité liés à toutes ces données et touchant à la fois à leur intégrité mais aussi à leur confidentialité car les flux qui transitent, voire résident, sur les serveurs de ces opérateurs sont susceptibles d'être sensibles (voir le paragraphe 5.3 « Sécurité des données et la protection du patrimoine scientifique »).

Les aspects immédiatement pratiques cachent un niveau de services des offres commerciales très faibles. Par exemple, ces opérateurs ne garantissent aucune sauvegarde. Ce qui veut dire qu'en cas de destruction accidentelle ou bien de dysfonctionnements des serveurs, l'utilisateur n'a aucune chance de récupérer ses données. La disponibilité de ces services n'est pas sans faille. L'accroissement de leur nombre d'utilisateurs est un facteur qui pèse très lourd dans le niveau de ressources nécessaires et le risque de pannes. Enfin, l'utilisateur ne peut compter sur aucun support. Il est un utilisateur anonyme parmi des millions.

4.3 Interaction avec des moyens tiers

On désignera par « moyens tiers » un ordinateur n'appartenant ni au laboratoire, ni à l'individu mais mis à disposition par un tiers. Il peut s'agir d'un ordinateur dans un café-internet, dans une conférence, dans un autre laboratoire, un hôtel etc.

Ce type d'usage peut paraître très pratique mais pose de sérieux problèmes. En effet, ces ordinateurs sont sous le contrôle d'intérêts qui ne sont pas du tout les nôtres. Il est très facile de les « piéger » de façon logiciel ou matériel pour enregistrer les actions d'un utilisateur et ainsi détourner des trafics ou voler des mots de passe et ensuite infiltrer nos réseaux et nos systèmes. Situation aggravée par le fait qu'en général les mots de passe ne sont pas régulièrement changés (voir le paragraphe 5.2 « La sécurité à l'entrée du réseau »).

Les réponses à l'enquête montrent que seulement 33% des personnes ne font jamais usage de terminaux en libre service. Pour les autres, l'usage se répartit dans diverses circonstances (autres laboratoires, conférences, cafés Internet, salles de formation). Les risques ne sont pas strictement équivalent suivant les lieux. Par exemple, le café Internet est de loin le plus risqué et pour les autres, le risque dépend du niveau de confiance qu'il n'est pas toujours aisé de mesurer. Il existe des exemples de prêt de matériel piégé par un organisme d'accueil.

4.4 Démêler les mélanges

Le mélange des sphères conduit directement à une situation dans laquelle chaque personne choisit sa solution parmi un certain nombre d'offres ou de tentations. Au bout du compte, plus personne ne saura où sont les données, les services, les moyens et même les utilisateurs. En somme, on finira par ne plus savoir de quoi dépend l'activité de recherche. Il est donc important de mettre en place des solutions pragmatiques et évolutives pouvant contrecarrer cette tendance et démontrer aux utilisateurs qu'ils ont intérêt à utiliser les solutions professionnelles qui sont mises à leur disposition.

4.4.1 Politique d'équipement

Tout d'abord, il est nécessaire de développer une politique d'équipement en ordinateurs portables pour les personnels qui ont un besoin de travail à distance. Notamment équiper correctement les doctorants qui souvent ne sont pas dotés d'ordinateur ou bien de matériel obsolète, même pour travailler en interne. Situation qui conduit inévitablement à l'usage d'un poste privé.

4.4.2 Hypermobilité et hyper-connectivité

L'accès à des ressources professionnelles devrait toujours se faire par un moyen sous la responsabilité de l'utilisateur et suivant les procédures définies par son service informatique. Cependant, il n'est pas toujours possible ou souhaitable de se déplacer avec son poste de travail portable (encombrement, poids...). La fourniture aux utilisateurs d'équipements hyper-mobiles (mini-PC, PDA, smartphone...) serait un facteur permettant à la fois de réduire les risques d'usages de postes de travail tiers ou privés et d'apporter un outil complémentaire pratique.

Lorsqu'on regarde un portable qui a un peu voyagé, on y trouve la trace d'une quantité importante de réseaux sans-fil qui se sont trouvés sur son itinéraire et éventuellement sur lesquels il s'est connecté. Par exemple : ceux des organismes dans lesquels il était en mission, celui de son fournisseur d'accès Internet à domicile, ceux de tous les aéroports visités, des gares, des conférences, des hotels, des bars, celui du voisin ou d'autres particuliers ou encore des pirates ainsi placés dans la situation de « l'homme du milieu », individu fortement connu en matière de sécurité informatique. On trouve donc là une preuve concrète du mélange des sphères et qui caractérise bien les mille et un tracas que doit rencontrer un utilisateur confronté à des circonstances de connexion toujours différentes.

Pour ces raisons, il serait très intéressant de les doter de moyens de connexion haut-débit par le biais du réseau téléphonique cellulaire (aujourd'hui communément appelés 3G et qui englobent aussi des offres Wifi). Il faudrait donc négocier ces abonnements au niveau de l'institut. Cela permettrait aux utilisateurs un maximum de flexibilité, d'autonomie, éventuellement de redondance et d'éviter de devoir « errer » à la recherche d'un point d'accès Wifi utilisable. Bien évidemment, il ne s'agit pas là d'une solution parfaite en termes de couverture géographique, mais de nature à réduire fortement l'usage de réseaux peu sûrs.
Aujourd'hui, l'hypermobilité existe déjà au sein de l'IN2P3 puisque environ 15% des personnes ont déclaré déjà utiliser un équipement hypermobile. 14% déclarent déjà utiliser le réseau 3G.

4.4.3 Explorer

Il existe des solutions permettant d'installer des systèmes d'exploitation sur des dispositifs tels que des clés USB. Ces solutions méritent d'être explorées car elles permettent aux administrateurs des services informatiques de fournir aux utilisateurs des systèmes professionnels, amorçables sur n'importe quelle machine, qu'elle soit professionnelle ou privée, sans risque de contamination

(systèmes symbiotes). Ces systèmes restant ainsi sous le contrôle des administrateurs, permettraient de séparer les deux types d'activités. De telles solutions pourraient aussi être favorablement utilisées pour les cas de sortie du territoire français. (voir le paragraphe 5.3.2 « Risques sur la confidentialité »)

4.4.4 Veille socio-technologique

Une veille technologique active doit être pratiquée afin que les équipes de support ne soient pas dépassées par les innovations technologiques et puissent y faire face le plus rapidement possible. Cependant, au-delà des aspects technologiques, il semble de plus en plus important de comprendre les comportements de la société face à l'offre numérique grand public parce qu'ils ont des incidences très directes sur la façon dont est perçue et utilisée l'offre numérique professionnelle.

4.4.5 Qualité du support

Développer un support de qualité est primordial pour faire la différence avec toutes autres prestations externes et permettant aux utilisateurs de se décharger d'une gestion informatique chronophage et pénible. Notamment la capacité de restaurer des fichiers perdus, d'individualiser l'aide ou les solutions, de résoudre, contourner rapidement des problèmes, répondre à des problèmes spécifiques de la recherche, etc.
Enfin, il est également primordial de mettre en ligne les applications que déploient les opérateurs commerciaux, qui nous manquent et qui attirent nos utilisateurs parce qu'elles s'avèrent très utiles pour leur activité.

5 Remise en cause de la sécurité du système d'information

Face au phénomène du nomadisme, la sécurité du système d'information est devenue beaucoup plus compliquée et les repères habituels ne sont plus suffisants. L'architecture traditionnelle déployée jusqu'ici un peu partout et notamment dans l'IN2P3 consiste en une protection périmétrique. C'est-à-dire l'ensemble des moyens informatiques connectés sur un même réseau, le réseau dit interne, lui même connecté par un seul point à l'Internet à partir duquel sont assurés les filtrages de l'extérieur vers l'intérieur et vice-versa.
Deux éléments changent profondément la donne. D'une part, désormais l'ensemble des moyens informatiques n'est plus sur le réseau interne, protégé des « agressions » externes, mais un peu partout, éparpillé sur l'Internet, dans un milieu incontrôlable et rendu hostile par une cyber-criminalité en hausse. C'est comme si le réseau éclatait. Chaque individu devient une singularité distincte et mouvante de ce réseau. D'autre part, la palette de fonctions nécessaires aux utilisateurs depuis l'extérieur s'élargit au point que l'on peut considérer qu'ils transportent leur bureau. (Voir chapitre 3 « Usages du nomadisme »).

Ces bureaux mobiles sont donc autant de points vulnérables qui exposent le système d'information.
Il est donc clair qu'une politique de sécurité sérieuse est un élément incontournable si on souhaite pouvoir fournir un service de qualité tout en minimisant les risques ou, en tout cas, les ramener à un niveau acceptable et gérable. Il est important de concevoir la sécurité comme un avantage bien compris par chacun pour apporter plus de services et de qualité.

5.1 Sécurité du poste de travail nomade

Lorsqu'un poste de travail devient nomade, il se trouve exposé plus fortement et plus souvent à

diverses menaces et notamment le vol ou la perte ainsi qu'aux risques d'infections virales.

5.1.1 Le vol

Même si le nombre d'ordinateurs volés (ou perdus) déclarés au sein de l'IN2P3 n'est pas très élevé (4 déclarés en 2009), il n'en reste pas moins qu'il s'agit d'un fléau en forte progression et qui est le second délit informatique après la production de virus. (2000 vols au CNRS par an*)*
Si le vol d'un portable est pénalisant pour l'utilisateur parce qu'il ne dispose plus de son outil de travail, les conséquences les plus importantes sont la perte des données qui n'auraient pas été sauvegardées, la divulgation d'informations confidentielles, l'utilisation de moyens d'authentification qui y seraient stockés.
Le risque de perte ne peut se traiter qu'en appliquant une politique de sauvegarde ou de synchronisation. (voir le paragraphe 5.3.1 « Risques sur l'intégrité des données »).

Pour les autres risques, il sera de plus en plus important de chiffrer les disques et éventuellement les équiper de dispositifs d'authentification de l'utilisateur au démarrage. (voir le paragraphe 5.3.2 « Risques sur la confidentialité »).

Il existe des dispositifs permettant de repérer géographiquement un ordinateur s'il est connecté à Internet. En cas de vol, s'il se présente sur le réseau, l'ordinateur sera repéré. Si ces dispositifs sont utiles pour casser sa valeur marchande, ils ne sont que de peu d'utilité pour limiter les risques qui nous préoccupent. De plus, cette méthode peut se heurter à des contraintes de respect de la vie privée puisque localiser un ordinateur, c'est aussi localiser son utilisateur. Pour ces raisons, il serait souhaitable d'évaluer plus finement l'utilité réelle de ces dispositifs et leurs conséquences avant d'en préconiser l'usage.
En dehors des solutions techniques précédemment citées, les meilleures parades consistent d'une part à inciter les utilisateurs à la vigilance (les informer sur la réalité du problème) et d'autre part à les informer sur la nécessité de déclarer les vols et la procédure à suivre en cas de vol ou de perte.

5.1.2 Risque viral

La mobilité des ordinateurs ne doit pas être un frein à la mise à jour de leur logiciel anti-virus, de leur système d'exploitation ou de leurs logiciels embarqués. En effet, un nouveau virus est très virulent dans les semaines qui suivent sont apparition car il bénéficie du retard de mise à jour des machines. Les machines nomades sont susceptibles de fréquenter des réseaux peu sûrs et de rester longtemps loin de leur base. Il est donc important que les divers composants soient le plus à jour possible sans attendre de revenir dans le périmètre géographique de l'unité. Si ces mises à jour peuvent être faites directement à partir des serveurs des éditeurs, il est fortement préférable qu'elles soient faites sur des réplications internes. En effet, sur des réseaux peu sûrs, il est parfaitement possible pour un pirate de rediriger les requêtes destinées aux serveurs des éditeurs vers ses propres serveurs, avec des conséquences catastrophiques pour l'ordinateur. D'autre part, une mise à jour sur les répliquas internes permet aux équipes de support de connaître l'état des postes de travail.

Pour cela, l'utilisation de connexions VPN peut être un outil précieux et fortement conseillé (voir le paragraphe 5.2 « La sécurité à l'entrée du réseau »).

Les ordinateurs portables professionnels fréquentent très souvent les réseaux domestiques des personnels et c'est donc une situation où le risque d'effet retard mentionné plus haut est très important. Par conséquent, même si les ordinateurs privés présents sur ces réseaux ne sont pas directement utilisés pour l'activité professionnelle, il est important, non seulement de sensibiliser les utilisateurs au risque viral sur leur réseau, mais aussi de les conseiller pour le choix de logiciels

anti-virus. Ici l'intérêt professionnel passe par une bonne gestion privée.

5.2 La sécurité à l'entrée du réseau

La méthode d'entrée sur le réseau interne depuis l'extérieur est primordiale à la fois par l'outil et par la méthode d'authentification et conditionne le niveau de risque d'intrusion.

5.2.1 Authentification

L'authentification par simple mot de passe est la méthode historique utilisée partout (toutes les unités l'autorisent). Pourtant elle est la plus risquée car son niveau de sécurité est faible parce qu'elle dépend de la qualité du choix de l'utilisateur, sa compromission peut être aisée, les systèmes qui acceptent cette méthode sont l'objet d'attaques permanentes (attaques par force brute). De plus, souvent le mot de passe n'est jamais changé (seulement 5 unités imposent un changement régulier des mots de passe).

Il y a quelques années, l'usage des mots de passe ne posait pas trop de problème car toutes les connexions étaient internes et les utilisateurs, en général, en avait qu'un seul. La situation a bien changé. Aujourd'hui une personne doit gérer une multitude de mots de passe pour accéder à une quantité grandissante de services dans leur activité professionnelle mais aussi dans leur usage privé d'Internet (ebay, Amazon, impôts...). Ou bien la personne est sérieuse et différencie ses mots de passe et dans ce cas il lui faut presque une base de données, ou bien elle est moins sérieuse et utilise toujours le même mot de passe quelque soit les circonstances et dans ce cas le niveau de risque est très élevé. Ce qui était très pratique au départ est en train de devenir un cauchemar qui s'accommode mal de situations nomades ! Pour toutes ces raisons, dans la situation actuelle il ne peut être que recommandé de forcer l'expiration automatique des mots de passe et évoluer vers d'autres méthodes plus sûres et plus pratiques.

13 unités déclarent déjà utiliser à divers degrés des méthodes à authentification forte qui combinent une authentification mutuelle de l'utilisateur et de l'application sur laquelle il se connecte et une cryptographie sérieuse. C'est le cas notamment des certificats électroniques. Compte tenu de l'enjeu que représente désormais le nomadisme et si l'on souhaite le développer sereinement et de manière optimale, il sera très important de s'assurer de l'usage des meilleurs protocoles d'authentification du moment. Pour cela, l'évolution vers ces méthodes d'authentification fortes doit être encouragée.

Il serait même intéressant d'évaluer des dispositifs matériels qui permettent de stocker et d'utiliser les éléments d'authentification afin de simplifier les procédures pour les utilisateurs (carte à puce, clé cryptographique, biométrie, calculette de mots de passe à usage unique ...).

5.2.2 Méthodes de connexion

Depuis quelques années, le moyen principal de connexion depuis l'extérieur vers les laboratoires est basé sur le protocole SSH et consiste à se connecter sur un serveur d'entrée pour y rebondir vers d'autres services internes.

Cette situation est en train d'évoluer puisque 12 unités déclarent également utiliser l'accès par la méthode VPN (Virtual Private Network) ainsi que 20% des utilisateurs. Le principe est différent puisqu'il ne s'agit pas de se connecter sur un serveur pour y rebondir, mais de se connecter sur le réseau pour ensuite y travailler comme de l'intérieur. Cette méthode se marie bien avec la problématique, déjà expliquée, d'éclatement du réseau. En effet, le VPN permet en quelque sorte de tisser un réseau virtuel par-dessus Internet et donc de ré-unifier les singularités en établissant un tunnel de communication entre l'utilisateur et le réseau interne.

Cette méthode présente aussi bien d'autres avantages : possibilité de mettre en place des filtrages

fins, segmentation en sous-réseaux, meilleure traçabilité, fonctionnalités potentiellement équivalentes à un usage interne, facilité pour les utilisateurs (on travaille de façon identique en interne et en externe), meilleure adaptation aux besoins individuels, mise à jour des systèmes ou anti-virus à partir des serveurs internes, prise de contrôle à distance, etc.

Il faut toutefois noter que le manque d'harmonisation des filtrages en sortie des réseaux depuis lesquels nos utilisateurs peuvent être amenés à se connecter peut parfois être un frein à l'usage de solutions de connexions à distance. Il est bien sûr impossible de provoquer cette harmonisation au niveau mondial, mais elle serait souhaitable au sein de l'IN2P3.

5.2.3 Réduire les risques d'intrusion

S'il est important d'assurer une sécurité optimale en entrée de réseau, il n'en reste pas moins qu'il est tout aussi important de s'équiper pour contrecarrer les tentatives d'intrusion qui pourraient se faire par le biais des moyens nomades.

Même si le poste de travail nomade est équipé d'un anti-virus, le risque de contracter un virus n'est pas nul. Même si on met en place des dispositifs d'authentification efficaces, le risque de compromission existe toujours. Il est donc important de mettre en place sur le réseau interne des dispositifs de détection d'intrusion destinés à repérer des trafics suspects. 11 unités déploient, ou sont en cours de déploiement, des moyens de détection d'intrusion.

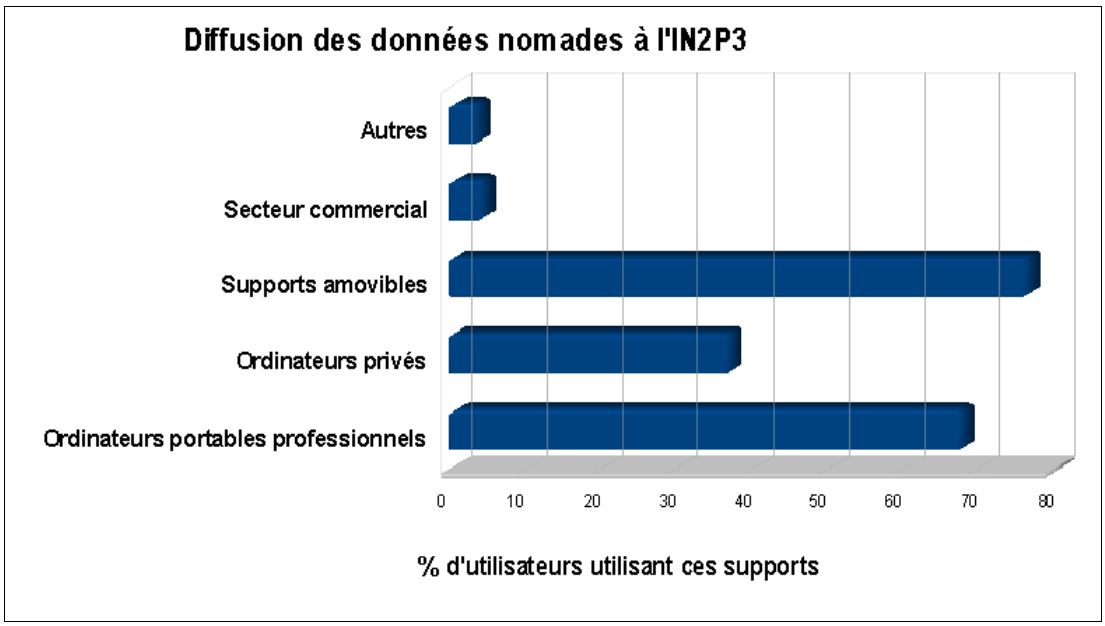
Le déploiement de nouveaux protocoles de contrôle d'accès au réseau (Network Access Control ou NAC) permettrait aussi de gagner en sécurité. Ces protocoles ont pour fonction de vérifier l'état d'un poste de travail lorsqu'il se connecte au réseau et ainsi de vérifier qu'il est conforme à la politique souhaitée (présence d'anti-virus par exemple).

5.3 Sécurité des données et la protection du patrimoine scientifique

Nous sommes passés en quelques années d'une situation où toutes les données étaient centralisées sur des serveurs bien identifiés dans les laboratoires à une situation bien moins déterministe et diffuse. Dans un premier temps, les données sont devenues mobiles avec les postes de travail. Puis, la mise sur le marché d'équipements amovibles, de taille réduite, mais offrant des capacités de stockage de plus en plus importantes pour un coût dérisoire a contribué à une dispersion encore plus floue et morcelée (clé USB, mini-disque externe...).

Parallèlement, des opérateurs commerciaux (Google, Yahoo...) mettent à disposition, gratuitement, des capacités de stockage importantes et accessibles de partout. Il s'agit là aussi d'un facteur qui, potentiellement, peut aggraver la dispersion des données, voire la perte de patrimoine scientifique. En effet, cet éparpillement, sans règle et suivant des options individuelles, aura des conséquences à long terme sur la capacité à regrouper l'ensemble des informations qui ont été produites sur les divers projets. Il y aura également des conséquences à plus court terme car des problèmes pratiques de gestion se poseront aux utilisateurs comme par exemple la nécessité de se préoccuper très directement de leurs sauvegardes.

Le graphique suivant montre la situation à l'IN2P3 d'après les déclarations des utilisateurs.



5.3.1 Risques sur l'intégrité des données

Avec la dispersion des données sur des supports non centralisés, se pose la question du maintien de leur intégrité, c'est-à-dire la capacité de les reconstituer en cas de destruction accidentelle, de perte ou de vol du matériel. A l'époque où tout était centralisé, l'ensemble des fichiers était sauvegardé périodiquement par des processus systèmes automatiques sous contrôle des équipes d'administration et l'opération était maîtrisable et maîtrisée, surtout pour les utilisateurs qui n'avaient pas à se préoccuper de cet aspect.

Aujourd'hui, l'intégrité repose beaucoup sur l'attitude des utilisateurs et de leur discipline dans leur gestion de données. Plus ils « sortent » de fichiers du système central et plus ils les dispersent sur différents supports, plus la situation se complique. La question qui se pose est : est-ce que tous les fichiers ont bien une copie à jour sur le système de gestion de fichiers central ? Ou, sous une autre forme, est-ce qu'il existe une sauvegarde de chaque fichier nomadisé ?

D'après les utilisateurs, la réponse est plutôt non. En effet, seulement 25% déclarent que les données présentes sur leur ordinateur portable sont totalement sauvegardées et 39% partiellement.

L'augmentation des capacités des supports nomades crée une tendance au déplacement de tous les fichiers des utilisateurs sur des moyens nomades et le risque ne plus avoir grand chose sur le système de fichiers central. Même la présence d'outils de sauvegarde ou de synchronisation sur les postes n'est pas une garantie absolue car, d'une part, il sera difficile de sauvegarder des supports amovibles et, d'autre part, il ne suffit pas d'avoir l'outil, il faut qu'il s'exécute très régulièrement. Les unités mettent presque toutes en œuvre des logiciels de synchronisation de fichiers (sauf 3), mais avec des solutions très disparates. Seulement 7 unités disposent de moyens de sauvegardes centralisées des postes nomades, là aussi avec diverses solutions logicielles.

Si les utilisateurs ont tendance à transporter beaucoup de données hors du laboratoire, c'est parce qu'ils y trouvent un intérêt pratique : pouvoir en disposer à tout moment dans leurs divers déplacements. Il s'agit aussi là d'un ancien réflexe du temps où les communications extérieur-intérieur étaient fortement limitées.

Pour cette raison, il est important de faciliter l'accès aux ressources depuis l'extérieur afin de permettre aux utilisateurs de les récupérer facilement et uniquement en cas de besoin. Mais cette mesure, si elle reste indispensable, n'est pas suffisante, car il est illusoire de penser que les données

resteront complètement centralisées.

De fait, une politique de sauvegarde des postes nomades est incontournable mais la difficulté principale ne réside pas tant dans des aspects purement techniques (quel logiciel, quel matériel) mais dans des aspects d'organisation (comment être sûr qu'un poste est sauvegardé très régulièrement, vers quoi on sauvegarde, quelles conséquences pour l'architecture centrale, etc...).

5.3.2 Risques sur la confidentialité

Un tiers des utilisateurs déclarent qu'il leur arrive de stocker des données à caractère sensible sur des supports nomades. En même temps, seuls 10% déclarent chiffrer totalement ou partiellement leur données. Ces chiffres montrent que le chiffrement des supports de stockage n'est pas encore entré dans les mœurs.

Pourtant, la dispersion des données conduit nécessairement à un accroissement des risques de violation de confidentialité par perte, vol ou parce qu'elles sont stockées sur des moyens appartenant à des intérêts tiers.

Certains organismes appliquent des politiques de sécurité très restrictives interdisant toute sortie de données ou de matériels pouvant en contenir. Cela tient à une culture ancienne et spécifique à un type d'activité. La culture des unités du CNRS est dans la plupart des cas très différente. Traditionnellement très ouverte notre activité est de plus en plus impliquée dans le tissu industriel et économique au travers de partenariats avec des entreprises du secteur privé, par exemple, pour qui la notion de confidentialité a une valeur vitale.

La solution à cet impératif de protection passe d'abord par la réduction du nombre de fichiers nomades au strict nécessaire surtout s'ils sont sensibles. Ensuite, il devient important de chiffrer les supports mobiles. Pour les ordinateurs, des tests sont en cours et les problèmes techniques sont surmontables. Mais l'organisation est plus compliquée car il faut que les équipes de support restent capables d'intervenir sur un poste chiffré, ce qui nécessitera la mise en place de procédures particulières de conservation des clés de chiffrement par exemple.

L'autre problème d'organisation concerne les postes susceptibles de sortir du territoire français, c'est-à-dire potentiellement tous. Les recommandations du fonctionnaire de défense stipulent de ne pas exporter un ordinateur chiffré pour, soit ne pas se mettre en contradiction avec les lois du pays, soit éviter de devoir donner sa clé de chiffrement au douanier qui peut avoir le droit de la réclamer et « d'ausculter » la machine. Ce qui signifie qu'un utilisateur doit pouvoir disposer d'un deuxième ordinateur. Évidemment cette situation est très compliquée car les utilisateurs n'ont en général pas ce luxe.

La seule solution envisagée aujourd'hui est que chaque unité dispose d'un ensemble d'ordinateurs communs qu'elle prête à ceux qui partent à l'étranger. (3 unités ont déclarées avoir ce type de procédure). Il s'agit-là d'une procédure très compliquée pour l'utilisateur. Il doit réserver une machine, qui doit être disponible, venir la récupérer le jour dit, et qui la trouve dans un environnement différent de celui dont il a l'habitude. La situation est aussi compliquée pour les équipes de support qui doivent gérer ce parc, réinitialiser les systèmes à chaque retour, adapter la machine à l'utilisateur (logiciels, moyens de communication et d'authentification à distance, car si la personne n'a rien sur son poste, elle devra pouvoir se connecter sur son unité).

Face à ces contraintes, les utilisateurs risquent soit de ne pas respecter les recommandations, soit de les respecter, mais en accentuant le mélange des sphères (utilisation d'un ordinateur privé ou de moyens tiers, éventuellement commerciaux (voir le chapitre 4 « Le mélange des sphères »)).

Si on souhaite pouvoir respecter les recommandations, il faudra trouver des solutions qui réduisent, au moins en partie, ces contraintes. Par exemple la fourniture de systèmes sur clé USB, pouvant

être démarrés indépendamment d'une installation sur la machine. (voir aussi le paragraphe 4.4 « Démêler les mélanges »).

Pour toutes ces raisons, il est important de définir une politique du chiffrement commune pour l'institut qui établira un cahier des charges à suivre pour la sécurisation des postes nomades.
Par exemple : doit-on chiffrer de façon matérielle ou logicielle, tout ou partie des disques, quels dispositifs minimaux doivent embarquer les nouveaux postes nomades, comment organiser le séquestre des clés de chiffrement, quelle posture par rapport aux sorties du territoire, etc...
Cette politique du chiffrement sera une référence aussi bien pour les administrateurs systèmes et réseaux que les utilisateurs et permettra de définir un contexte adapté et concerté pour le déploiement des postes nomades. Son évolution dans le temps permettra également d'adapter nos réponses à l'évolution des risques.

6 Le support du nomadisme

Les 16 unités qui ont répondu totalisent environ 1550 portables. Ce qui correspond à un taux d'équipement nomade d'environ 60%. Cela signifie que plus de la moitié du parc informatique des unités est susceptible de sortir des périmètres internes et que chacun de ces postes a une « vie » extérieure indépendante. L'histoire d'un poste échappe de plus en plus aux équipes de support et la résolution des dysfonctionnements peut devenir très complexe et chronophage. Et le temps d'intervention et d'immobilisation dans l'unité est de plus en plus réduit puisque les portables sont, par définition, mobiles.

La situation est encore plus compliquée lorsque les utilisateurs sont complètement gestionnaires de leur poste professionnel, sans intervention du service informatique. Cela peut arriver par exemple parce que le système d'exploitation n'est pas pris en compte par le service informatique. Ou encore, avec des machines d'acquisition, éventuellement financées par une autre unité, avec des systèmes spécifiques et mobiles.

Le support devient plus difficile et pourtant de sa qualité dépend fortement la capacité que nous aurons à mieux maîtriser les enjeux du nomadisme, notamment pour réduire les risques de dispersion de nos activités vers des intérêts qui ne ne sont pas les nôtres et pas forcément compatibles avec le milieu de la recherche. La qualité de service et du support feront la différence.

6.1 Influence sur le support des changements d'habitudes engendrées par le nomadisme

Si le nomadisme est un facteur d'évolution technologique, il a enclenché également une évolution de plus en plus perceptible des habitudes de travail et plus particulièrement un étalement des plages horaires de travail.

En effet, les horaires de travail classiques et communs ne sont plus respectés, soit parce les utilisateurs travaillent depuis chez eux nuits et week-ends, soit parce qu'ils sont sur des expériences externes impliquant des communications avec leur base à tout moment, soit parce qu'ils sont à l'étranger avec un décalage horaire important. Même dans les laboratoires qui ferment pendant des périodes de congés bloquées, l'activité extérieur-> intérieur reste élevée. L'activité en provenance de l'extérieur est devenue au fil des années quasi-continue, nuit et jour, sept jours sur sept et il est probable que les choses s'accentuent en terme de nombre d'utilisateurs.
Ceci a une conséquence directe sur le niveau nécessaire de disponibilité des services. Certes le nomadisme n'est pas le seul facteur qui oblige le maintien du niveau de disponibilité mais il

accentue notablement certaines contraintes. Par exemple, les périodes possibles de maintenance pour les équipes d'administrateurs systèmes et réseaux (ASR) deviennent très étroites. Ou encore, l'utilisateur est d'autant plus sensible à un problème lorsqu'il est loin parce que, d'une part, il est « aveugle » sur l'origine des problèmes, leur gravité, leur durée et d'autre part, à distance, son activité lui impose souvent des contraintes externes qui s'accommodent mal d'un service peu fiable et de délais trop long d'indisponibilité.

Ces facteurs entraînent la nécessité de mettre en place des moyens redondants mais aussi de développer une démarche qualité permettant une meilleure gestion globale par une amélioration continue des processus. Il entraîne également une attention soutenue et une capacité d'intervention rapide des équipes de support. 10 unités ont déclaré qu'il serait intéressant que les ASR soient équipés de moyens de connexion 3G. En effet, les ASR sont eux-mêmes mobiles et la capacité de disposer d'une liaison « facile », à tout moment, leur permettrait d'être indépendants de moyens tiers et d'assurer un meilleur suivi de leur exploitation, même à distance.
Comme nous l'avons dit plus haut, le nomadisme favorise les interactions entre les diverses sphères et les utilisateurs se voient proposer des alternatives aux moyens strictement professionnels. Ils ont donc désormais beaucoup plus la possibilité de choisir des solutions qu'auparavant, lorsque l'informatique était centralisée. Cet état de chose rentre en collision frontale avec le travail des administrateurs systèmes et réseaux. Ils sont pris entre des utilisateurs qui s'approprient rapidement, et séparément, les technologies qui leur sont désormais accessibles, et la perception qu'ils ont de la nécessité de maintenir la cohérence globale et la qualité de service. Ils sont également conscients des remises en cause, des risques et des contraintes que cela suscite. Bien souvent, les administrateurs systèmes et réseaux doivent « faire la police », situation qui peut rendre les rapports plus difficiles avec les utilisateurs.

La veille technologique et la formation doivent faciliter la situation en permettant aux ASR de mieux anticiper et mieux connaître les technologies impliquées par le nomadisme. Cette veille est un peu particulière, car elle doit aussi observer les évolutions qui sont d'abord destinées aux particuliers et en évaluer l'utilité et l'impact dans l'activité professionnelle. Par exemple, lorsque les ordinateurs portables sont apparus, ils étaient, du fait de leur coût, plutôt destinés à une clientèle professionnelle. Aujourd'hui, la plupart des technologies liées à la mobilité sont d'abord ciblées sur le grand public et « fréquentent » ensuite la sphère professionnelle. Par exemple, les smartphones, les réseaux Wifi communautaires, les offres des opérateurs commerciaux.

6.2 L'utilisateur administrateur

De plus en plus d'utilisateurs sont administrateurs de leur poste et ont donc la possibilité de modifier le système sans que les équipes des services informatiques soient au courant, voire même d'accord. Aujourd'hui 14 unités sur 16 accordent des privilèges administrateurs aux utilisateurs et 70% d'entre-eux déclarent qu'ils possèdent les droits administrateurs sur leur portable professionnel.

La question du privilège administrateur est un point important de débat entre les utilisateurs et les administrateurs systèmes et réseaux. Pour ceux-ci, la situation idéale voudrait que les utilisateurs ne disposent pas du privilège administrateur sur leur poste afin que son paramétrage, notamment d'un point de vue sécurité, ne soit pas modifié. Pour l'utilisateur, sa capacité à débloquer un problème imprévu lorsqu'il est loin de sa base est essentiel, sous peine de compromettre son activité. On peut faire la comparaison avec une voiture de fonction utilisée en mission dont il serait interdit d'ouvrir le capot en cas de panne.

Si 70% des utilisateurs ont le privilège administrateur seulement 57% déclarent connaître les obligations d'un tel privilège et 60 % connaître les problèmes de sécurité qui y sont liés. Ceci

montre que si les contraintes de fonctionnement efficaces poussent à accorder le privilège administrateur aux utilisateurs il n'en reste pas moins qu'il est important qu'ils en connaissent les règles. La sensibilisation et la formation sont des outils incontournables pour changer cette situation, pour minimiser les risques et améliorer les rapports avec les équipes de support sur ce point. Un utilisateur qui se voit accorder le privilège administrateur devrait obligatoirement suivre une séance de formation à l'usage d'un poste de travail. Cette séance notamment devrait être insérée dans le parcours du nouvel entrant. Le contenu de cette formation pourrait être élaboré globalement pour l'IN2P3.

6.3 Le support à distance

Comment fait un utilisateur lorsqu'il est à l'extérieur du périmètre géographique de son unité, par exemple en mission, pour être dépanné sur un problème touchant ses moyens informatiques nomades ?

A cette question, les réponses des utilisateurs sont très diverses. Par exemple, ils interrogent. leurs collègues informaticiens de leur unité par mail ou par téléphone. Il peuvent également faire appel à du personnel sur leur lieu de travail. Et s'il ne peuvent avoir de réponses par ces moyens, ils se « débrouillent », tentant de résoudre leur problème par eux-mêmes (et c'est notamment pour cela qu'ils souhaitent disposer du privilège administrateur).

La prise de contrôle à distance des postes nomades est une solution qui mérite d'être développée car elle permet aux équipes de support de se connecter sur ces postes nomades où qu'ils se trouvent. 4% des utilisateurs déclarent utiliser cette méthode qui est déployée par 4 unités. Son avantage est de permettre au support d'intervenir directement sur le problème et d'avoir une chance de le débloquer rapidement. Son développement permettra d'ajouter une pièce importante dans la qualité de service offerte en assurant cette fois le « cordon ombilical » dans le sens unité -> poste nomade.

Les propositions faites dans les paragraphes précédents consistant à plus déployer des solutions d'hyper-mobilité et d'équiper les utilisateurs de capacité 3G sont aussi de nature à leur fournir des moyens redondants, au moins pour communiquer avec leur base, en cas de défaillance de leur poste de travail ou des capacités de communication plus classiques.

6.4 Accueil des visiteurs sur nos réseaux

Nos unités accueillent en permanence des personnes externes. Il est important que nous soyons en mesure de leur fournir une connectivité vers Internet de la même manière que nos propres ressortissants souhaitent pouvoir en disposer lorsqu'ils sont en déplacement dans d'autres unités. C'est un aspect qui touche à notre image de marque.

Treize des seize unités qui ont répondu à l'enquête pour les services informatique permettent aux visiteurs de se connecter à partir de leur réseau.

Compte tenu des origines diverses et variées de ces postes visiteurs, il est impossible de connaître leur niveau de sécurité et notamment la présence ou non de logiciel anti-virus efficaces. Aussi ces postes sont en général connectés dans des sous-réseaux dédiés, sans liaison avec le reste du réseau interne. Seulement 8 unités ont mis en place un filtrage de ces réseaux visiteurs vers l'extérieur. Pourtant il est important de limiter les possibilités en sortie au strict nécessaire afin de réduire le risque de trafics « agressifs » vers des tiers et impliquant notre responsabilité juridique. Il serait bon que la liste des services ouverts en sortie pour les visiteurs soit réfléchie de manière commune à l'ensemble des unités (au sein du groupe sécurité par exemple).

Authentification des visiteurs

Quelques unités n'imposent aucune forme d'authentification permettant de contrôler l'accès à leur

réseau visiteurs. Il suffit de capter le signal Wifi de ce réseau pour s'y connecter. Les autres utilisent diverses méthodes allant de la clé secrète partagée au portail captif permettant d'autoriser uniquement des personnes connues. Cette dernière méthode (mise en œuvre par 8 unités) est intéressante parce qu'elle est de plus en plus utilisée dans le monde et par conséquent de plus en plus connue des visiteurs potentiels. Elle est simple pour l'utilisateur (un navigateur web suffit), indépendante de la technique d'implémentation utilisée et les éléments d'authentification peuvent être délivrés rapidement. Le déploiement d'une telle solution dans chaque unité de l'IN2P3 permettrait de présenter une méthode d'accès au réseau pour les visiteurs identique, facile et déjà connue de la plupart.

Eduroam

Eduroam est un service déployé dans le milieu de l'enseignement supérieur et de la recherche et permettant un accès sécurisé à l'Internet à partir d'un réseau sans-fil pour des personnes invitées. Le principe consiste en une architecture qui permet à toute personne dont l'établissement est membre d'Eduroam de pouvoir se connecter à l'Internet depuis le réseau de tout autre membre et ce, avec les éléments d'authentification liés à son propre site, sans formalités supplémentaires et sans avoir à se faire connaître explicitement.

Pour proposer ce service à nos visiteurs, il faudrait donc, a priori, que chaque unité soit membre d'Eduroam. La première question qui se pose donc est : « est-ce que c'est souhaitable ? » Est-ce que le fait d'appartenir au milieu éducation/recherche doit donner un sésame sur nos réseaux, transformant ainsi nos laboratoires en potentiels fournisseurs d'accès pour une population bien plus large que celle qui la concerne? La réponse est plutôt non, ce n'est pas la vocation de nos unités. En revanche, ce rôle de fournisseur d'accès correspond mieux aux campus universitaires qui proposent de plus en plus Eduroam. Les visiteurs présents dans les locaux des unités couvertes par le service réseau du campus peuvent en bénéficier sans que l'unité elle-même en soit adhérente.

Il faut bien noter que d'offrir le service Eduroam n'enlève pas la nécessité de fournir un autre moyen d'accès. En effet, aujourd'hui, un grand nombre de visiteurs n'a pas accès à Eduroam soit parce que leur établissement, bien que éducation/recherche, n'est pas adhérent, soit il l'ignore, soit il n'appartient pas à ce monde. Il reste donc important de maintenir une autre solution qui peut être suffisante s'il n'est pas possible de bénéficier des services du campus.

Pour la situation inverse, c'est-à-dire la possibilité pour nos utilisateurs de bénéficier d'Eduroam lorsqu'ils sont à l'extérieur de leur unité et que le service est disponible, la solution la plus logique consiste aussi à utiliser l'adhésion à Eduroam du campus universitaire de rattachement des unités (création de comptes Eduroam auprès des services réseau universitaire).

Aujourd'hui, aucune unité de l'IN2P3 ne déploie de service Eduroam.

7 Comment mieux répondre au nomadisme ?

Ce chapitre a pour but de résumer les propositions qui ont été faites dans les chapitres précédents en les résumant, associant et complétant. Pour chaque proposition figurent des pointeurs vers les paragraphes concernés qui contiennent tous les détails utiles à la compréhension.

1) **Politique d'équipement de base**

L'ordinateur (fixe ou portable) est devenu un outil de base dans l'activité professionnelle des agents. Des carences en équipement (absence ou obsolescence) induisent directement l'usage de moyens privés et par là même la nomadisation d'activités professionnelles sans contrôle. Il est donc essentiel que tout personnel puisse disposer des moyens informatiques en rapport avec son activité et avec l'état de l'art afin de minimiser le mélange des sphères (§4). Les doctorants notamment sont souvent pas ou mal équipés, contraints à utiliser leur propre ordinateur avec à la clé des problèmes de support, de dépannage, de licences, de compatibilité, etc. De fortes incitations doivent être faites auprès des groupes de recherche et des unités pour que tout nouvel arrivant puisse être correctement équipé. Une dotation pourrait être octroyée par l'IN2P3 pour chaque doctorant arrivant afin de financer une partie de son équipement et montrer ainsi une volonté politique de résorber ces problèmes.

2) Intégrer l'hypermobilité (§ 4.4.2)

Il existe dans l'IN2P3 des personnes très en pointe dans les technologies hyper-mobiles (smartphone, liaison 3G). Les expériences du passé ont déjà montré qu'il y a toujours des « pionniers » et que les configurations qui pouvaient être considérées comme un luxe à une époque deviennent très rapidement la norme (par exemple les ordinateurs portables).
Commencer à introduire ces technologies pour ceux qui en ont le plus besoin permettra des retours d'expériences forts utiles et sera une façon pour les équipes systèmes et réseaux de mieux appréhender ce monde. Toutefois, la prise en compte des demandes des utilisateurs doit être équilibrée par leur responsabilisation pour les modérer face aux effets très négatifs que risque de produire l'usage anarchique de technologies sans validation ni concertation.
Etre connecté depuis partout est un fait de société qui déborde largement dans notre activité professionnelle. De plus en plus, les personnels, dans leurs déplacements, rencontrent la nécessité de se connecter depuis toutes sortes de lieux et de multiples possibilités s'offrent à eux avec des moyens techniques divers et variés, professionnels ou non. Ces possibilités cachent des problèmes de complexité (les méthodes sont différentes) ou de sécurité mal maîtrisés ou encore peu connus, notamment lorsque apparaissent de nouveaux concepts (réseaux communautaires par exemple).
Pour cela, et afin de pouvoir proposer un moyen et une méthode de connexion plus homogènes et plus sûrs, il serait souhaitable de négocier pour l'institut des abonnements groupés au réseau de téléphonie cellulaire haut-débits (aujourd'hui communément appelés 3G) et les mettre à disposition des personnes les plus mobiles. Cela ne garantirait pas une couverture absolue mais permettrait de rejeter à la marge le recours à d'autres types de réseau non maitrisés.

3) **Qualité de service et qualité du service (§ 6).**

L'accès aux ressources centrales depuis partout est devenue très sensible à la disponibilité

des moyens. Une attention particulière doit être portée non seulement à la mise à disposition de moyens d'accès distant mais aussi à leur fiabilité, disponibilité et redondance.
Il est à noter que ces aspects sont attisés par l'apparition de crises (telles que flambée du pétrole, grippe A) qui ont montré que les décideurs institutionnels du pays ont bien assimilé que la technologie permet aujourd'hui le télétravail dans des conditions acceptables et qu'ils considèrent qu'il s'agit là d'une possibilité pour contourner ou minimiser les risques inhérents à nos modes de vie.

La qualité du service est aussi un facteur essentiel à produire vers les personnels nomades afin de gérer de façon la plus efficace possible tous les problèmes pouvant intervenir dans cette situation. Doivent être notamment développées les possibilités de support à distance et les démarches qualité pour améliorer les divers rouages.

4) <u>Mettre en place des applications collaboratives</u>

L'utilisation de moyens externes de types applicatifs ou matériels représente un risque de dispersion, voire de perte de contrôle, des moyens nécessaires à l'activité scientifique. Face aux offres en matière d'outils collaboratifs (messagerie, agendas, planifieurs...) des opérateurs commerciaux (§ 4 et §4.2), il devient de plus en plus nécessaire de statuer sur la mise en place, dans le milieu de la recherche, de ces outils utiles et pratiques qui manquent à nos utilisateurs. Il convient donc de lancer une étude et réaliser un cahier des charges afin de bien cibler quelles applications sont pertinentes et comment il faut les déployer. La capacité de maintien et d'évolution des solutions sera un facteur très important à considérer afin de ne pas être dépassés à nouveau à court terme.

5) <u>Adapter la sécurité</u>

Le nomadisme implique obligatoirement la sécurité. Il s'agit de résoudre une équation délicate consistant à offrir de plus en plus de fonctionnalités à nos utilisateurs distants, protéger notre patrimoine scientifique et barrer l'accès aux « indésirables ». L'enjeu est simple : si cette équation n'est pas résolue de façon optimale la capacité même de fournir des fonctions nomades sera fortement altérée et indubitablement, l'activité de recherche en général serait perturbée.

Une politique globale de sécurisation du poste nomade doit être créée au niveau de l'institut. Elle comprendra trois volets : la politique anti-virale (§ 5.1.2), la politique de chiffrement (§ 5.3.2), la politique de sauvegarde (§ 5.3.1). Il ne s'agit pas là forcément d'opter pour les mêmes outils techniques mais de mettre en place le cadre minimal d'organisation et de fonctionnalités que ces outils doivent respecter.

De plus en plus d'utilisateurs sont connectés sur le réseau interne depuis l'extérieur avec pour conséquence un risque d' inadéquation grandissante des principes de sécurité mis en place à une époque où la situation était plus simple. Par conséquent la sécurité doit être re-considérée globalement face aux nouveaux risques de manière à associer authentification forte, architecture, capacité de filtrage, détection d'intrusion, analyse de conformité, traçabilité. Il s'agit de prendre le problème par une analyse et un traitement du risque dans le but de le réduire à un niveau résiduel acceptable.

6) Mettre en place un observatoire des technologies numériques nomades pour la recherche

Le monde du nomadisme numérique évolue très vite aussi bien du point de vue du matériel, des systèmes, des offres mais aussi, et peut-être surtout, par son imprégnation dans la société qui produit inévitablement dans notre activité professionnelle très spécifique des effets de bord dont on ne mesure pas toujours facilement les effets à moyen et long terme.
La création d'un observatoire des technologies numériques nomades pour la recherche permettrait de mutualiser les efforts de veille et d'évaluation. Il permettrait le développement d'une expertise en matière de nomadisme numérique, de mieux appréhender les évolutions et leurs interactions avec notre activité, d'éviter les mauvaises pistes. Il permettrait également de ne pas seulement voir le côté problématique des mutations technologiques mais d'en tirer aussi un bénéfice pour la recherche.
Cet observatoire pourrait être constitué de membres de l'IN2P3 mais aussi plus largement du CNRS, puisque la problématique n'est pas limitée à notre seul institut. Ces personnes devraient être volontaires pour accorder une partie de leur temps à cette activité, en accord avec leur unité, et bien identifiées par l'IN2P3 (ou le CNRS).
Ses missions seraient :

- Développer une expertise dans le domaine des technologies nomades
- Assurer une veille permettant de produire des documents et synthèses au bénéfice de tous
- Comprendre l'impact des évolutions sur notre activité scientifique et en extraire les facteurs pouvant faciliter directement ces activités (surveillance d'expériences, mobilité d'expériences, etc)
- Evaluer les solutions, les tester, les proposer
- Encadrer ou participer à des études
- Associer les utilisateurs

Cette idée, émise dans le cadre de ce rapport sur le thème du nomadisme mériterait certainement d'être étendue. En effet, les mêmes types de problèmes ou d'interrogations se posent, ou se poseront, sur un éventail de technologies bien plus large que celles qui concernent le nomadisme. Un observatoire des technologies numériques (en général) permettrait de favoriser une meilleure reconnaissance de l'activité de veille technologique, d'optimiser l'intégration des nouvelles technologies numériques dans l'activité scientifique et de disposer d'un outil d'aide à la décision.