

Avis du Comité économique et social sur la «Communication de la Commission au Conseil, au Parlement européen, au Comité économique et social et au Comité des régions — Sécurité des réseaux et de l'information: Proposition pour une approche politique européenne»

(2002/C 48/07)

Le 7 juin 2001, la Commission européenne, conformément à l'article 262 du traité, a décidé de consulter le Comité économique et social sur la communication susmentionnée.

La section «Transports, énergie, infrastructures, société de l'information», chargée d'élaborer les travaux du Comité en la matière, a désigné comme rapporteur M. Retureau. La section a adopté son avis le 6 novembre 2001.

Lors de sa 386^e session plénière des 28 et 29 novembre 2001 (séance du 28 novembre), le Comité économique et social a adopté le présent avis par 113 voix pour, 2 voix contre et 3 abstentions.

1. Introduction

1.1. Le développement des réseaux internes aux entreprises et aux administrations et autres organismes, ainsi que les connexions des précédents et des particuliers à l'internet, se poursuit à un rythme exponentiel; la saturation serait proche sans l'essor prochain de l'internet rapide ⁽¹⁾ et la mise en place engagée d'un nouveau système d'attribution de noms de domaines de premier niveau.

1.2. La société, l'économie, l'administration, la sécurité nationale, civile et militaire, sont devenues et seront de plus en plus dépendantes du bon fonctionnement et de la fiabilité des réseaux et de leurs interconnexions, de la largeur de leur bande passante, ainsi que de l'intégrité de l'information qu'ils contiennent et, dans nombre de situations, de la confidentialité des données ou de l'exacte identification des personnes en présence.

1.3. La sécurité des réseaux et des communications constitue désormais une question stratégique de la plus haute importance, qui nécessite une politique coordonnée et cohérente entre les pays membres de l'Union et au niveau global.

1.4. La Commission procède dans sa communication à une analyse très fouillée des problèmes posés et de la situation, que le Comité estime bien documentée, et elle formule des propositions d'action.

2. Les propositions de la Commission

2.1. La Communication de la Commission vise à la réalisation d'une approche commune des questions de sécurité des réseaux et de la transmission des informations en Europe. Il

s'agit de promouvoir un niveau équivalent de protection dans chacun des pays membres, une interopérabilité des systèmes, les missions de sécurité publique indispensables sur Internet et le rôle régulateur des États membres.

2.2. Il s'agit d'assurer une sorte de «service minimum» de la sécurité sur les réseaux et sur les connexions des particuliers à l'internet, sur les connexions des réseaux entre eux, et de développer une culture de la sécurité afin de promouvoir une prise de conscience générale des problèmes et des solutions.

2.3. C'est le maillon le plus faible qui détermine la sécurité de l'ensemble, et l'apparition progressive des liaisons à haut débit (ADSL, câble) et du branchement permanent, y compris des particuliers, sur l'internet fait naître de nouvelles exigences en matière de protection; il en va de même avec le commerce électronique, où les données personnelles et les références de paiement des consommateurs doivent être protégées, de même que les données personnelles des citoyens avec les progrès de la e-administration.

2.4. Un cadre pénal suffisamment harmonisé est également nécessaire pour que les délits d'intrusion, de détournement des données et informations ou la prise de contrôle de réseaux par des pirates ou la dissémination volontaire de virus soient définis et sanctionnés de manière équivalente dans chaque pays.

2.5. La création d'un système européen d'alerte et d'intervention est proposé, et la Commission insiste sur le besoin de formation et d'information, dans les entreprises et auprès des particuliers, qui constitue le point focal de la Communication.

(1) Norme Ipv6 permettant 6 000 milliards d'adresses IP.

2.6. Enfin, la proposition est articulée autour de l'objectif prioritaire de la protection de la vie privée et de la confidentialité des données individuelles des citoyens et des consommateurs.

3. Observations du CES

3.1. Observations générales

3.1.1. Le Comité partage pleinement les analyses et les arguments justifiant une politique cadre européenne de la sécurité des réseaux et de l'information, et estime les actions proposées généralement pertinentes, sous réserve de quelques observations et suggestions particulières.

3.1.2. Le réseau Internet n'a pas été conçu pour le commerce électronique, les contrats, la vente de contenus protégés par le droit d'auteur (musique, images et films), les transferts de capitaux et autres opérations économiques qui exigent des sécurisations spécifiques; dans son utilisation initiale, militaire et universitaire, le chiffrement avec des clés longues dans le premier cas et la publication de résultats d'expériences ou de bases de données scientifiques en clair dans le second, répondaient aux besoins. Pour des raisons de sécurité nationale, le chiffrement «fort» était souvent interdit aux particuliers jusqu'en 2000 dans nombre de pays essentiellement non européens, ainsi que l'exportation de certains programmes. La Commission a heureusement donné une impulsion au développement et au commerce des outils de sécurisation indispensables aux entreprises et aux administrations pour la transmission de données confidentielles en ligne.

3.1.3. Une utilisation «libertaire» de l'internet s'est développée par la suite, puis commerciale, financière, technologique et industrielle, ludique, sans compter les sites pornographiques qui génèrent d'importants revenus, et sont avec les jeux en ligne, à la source d'évolutions technologiques considérables notamment en matière de qualité d'image et de haut débit, ou de systèmes de paiement sécurisés, anonymes ou non.

3.1.4. Tous ces modes d'utilisation continuent de coexister et d'autres usages se profilent. Mais une part croissante des réseaux et de l'internet constituent des piliers du fonctionnement de la société et de l'économie, contribuent de manière décisive au développement social et à la sécurité nationale et demandent une sécurisation en proportion de la nature des données transmises et des opérations effectuées, dans le respect de la vie privée et sans remettre en cause ce qui est au

fondement même de l'internet, c'est-à-dire la circulation libre d'informations et l'échange ouvert de données, d'idées, de résultats scientifiques, etc.

3.1.5. Pour le Comité, il devra donc toujours exister une proportionnalité entre les mesures de sécurité adoptées et leur coût, la nature et l'importance des données et opérations protégées, les catégories d'utilisateurs concernés.

3.1.6. Le Comité partage d'une manière générale la présentation des risques potentiels et les solutions proposées par la Commission. Il partage aussi le point de vue selon lequel la sécurité est une question dynamique, qui demande une adaptation, des ajustements permanents, en fonction des évolutions des technologies, des logiciels et des risques. C'est pourquoi il suggère que la consultation et le dialogue engagés, à l'occasion de cette communication, avec les industries, les utilisateurs et les responsables de la sécurité des réseaux prennent un caractère permanent, ou qu'il y soit procédé périodiquement. La société civile organisée devrait y être pleinement associée, tant en raison de l'impact d'une politique de sécurité des réseaux et des communications sur certains des droits fondamentaux des citoyens que sur les activités économiques et sociales et l'administration.

3.1.7. Dans ses avis récents sur «la cybercriminalité»⁽¹⁾ et sur «la protection de l'enfance sur Internet»⁽²⁾, le Comité a déjà exprimé les principes essentiels qu'il soutient en vue de lutter contre l'utilisation de l'internet à des fins délictueuses ou criminelles tout en rejetant la censure, la surveillance généralisée et les entraves à la liberté d'expression et de communication sur le réseau global. L'internet n'est cependant pas en dehors du droit.

3.1.8. Le Comité estime que la sécurité des usagers individuels et des consommateurs, dans toutes ses dimensions, devrait occuper une place plus centrale dans la réflexion de la Commission et dans la stratégie européenne. Même si une attaque virale contre l'ordinateur d'un particulier n'a pas de

(1) Avis sur la Communication de la Commission au Conseil, au Parlement européen, au Comité économique et social et au Comité des régions — Créer une société de l'information plus sûre en renforçant la sécurité des infrastructures de l'information et en luttant contre la cybercriminalité (CES 1115/2001) (pas encore publié au Journal officiel).

(2) Avis du CES en cours d'élaboration sur un programme pour la protection de l'enfance sur Internet.

conséquence majeure du point de vue des intérêts économiques directs ou de la sécurité collective, il faut rappeler que certaines attaques se font à grande échelle, transitent par les postes clients, peuvent être montées en épingle par les médias parfois hors de proportion avec la réalité du danger encouru, ce qui réduit fortement la confiance des citoyen(ne)s envers les avantages et l'utilité de l'internet. Cela pèse considérablement sur le potentiel de développement du commerce électronique et du e-business en général, et sur la création d'emplois nouveaux.

3.1.9. Si la protection de la vie privée et des données personnelles sont des objectifs prioritaires, les consommateurs ont en outre le droit d'être protégés de manière réellement efficace contre le profilage nominatif abusif par «espioniciels» (spyware et web bugs) ou par d'autres moyens. La pratique du spamming (envois massifs de messages non sollicités) qui découle souvent de ces abus devrait aussi être efficacement freinée. Ces intrusions ont un coût pour les victimes (1).

3.1.10. La protection de la vie privée doit s'appliquer à tout le monde dans le milieu économique et commercial et par-là même être étendue aux salariés et autres collaborateurs d'une entreprise. Les règles internes de sécurité devraient être négociées entre les partenaires sociaux et être bien connues de tous dans l'entreprise, dans le respect du cadre légal ou jurisprudentiel du pays membre. Il faut à cet égard souligner l'importance d'une application uniforme de telles dispositions, conformément à la Charte des droits fondamentaux de Nice, et également en référence à la Recommandation des garants européens relative à la vie privée et à la Directive 95/46/CE sur la protection des données personnelles.

3.1.11. Il apparaît donc indispensable de donner aux particuliers et aux entreprises des moyens juridiques plus efficaces de mise en cause de la responsabilité pécuniaire des opérateurs et des fabricants de logiciels en cas de défaillances graves de sécurité et de protection des données qui leur soient imputables, au titre de la responsabilité du fait des produits (2).

3.1.12. La Commission devrait, selon le Comité, mieux valoriser et faire connaître également le rôle positif en termes de ressources et de protection que représente l'open source, c'est-à-dire les systèmes d'exploitation et les logiciels de réseaux et de communication gratuits et librement modifiables par les utilisateurs. La communauté des programmeurs de l'open

source réagit rapidement pour corriger les failles et problèmes, et un important secteur économique de services aux entreprises s'est développé autour de ce concept, soutenu par certains géants de l'industrie informatique. Un grand nombre de serveurs dans le monde fonctionnent avec ces logiciels de manière généralement sûre et stable, alors qu'il arrive parfois que certains logiciels propriétaires ne soient corrigés qu'avec un retard préjudiciable aux usagers, ou que de nouvelles versions de ces derniers comportant de nouvelles fonctionnalités soient mises hâtivement sur le marché. Les raisons de compétition commerciale ou la recherche à tout prix de la nouveauté prédominent parfois sur une culture de la sécurité, qui doit être renforcée chez tous les auteurs de logiciels, commerciaux ou gratuits, afin qu'elle soit vraiment intégrée aux produits dès leur conception.

3.1.13. De plus, les systèmes de gestion et programmes propriétaires, dont le code source n'est pas publié, n'offrent pas de ce fait de garantie suffisante de sécurité et de protection de la vie privée, surtout avec les enregistrements de licences et le chargement de patches (correctifs et mises à jour) effectués par l'internet, qui peuvent être détournés pour collecter des informations sur les systèmes client et serveur (architecture et contenus, listes d'adresses et connexions). Le Comité estime que toutes les pratiques allant au-delà du simple enregistrement du nom et de l'adresse du propriétaire de la licence du logiciel pour lui donner une clé d'activation ou un code d'accès temporaire à des services constitueraient une intrusion et devraient être prohibées.

3.1.14. Les logiciels libres (free: gratuits) assurent aussi, une forme de saine concurrence vis-à-vis des tendances monopolistes du marché des logiciels et du marché en plein développement des services de réseau.

3.1.15. La licence publique générale [GPL (3)] devrait être reconnue et respectée. Avec l'internet, le Comité estime que des approches et des règles spécifiques devraient être développées en matière de propriété intellectuelle en ce qui concerne les logiciels et les contenus accessibles ou échangeables via l'internet. Il n'est que trop facile, par exemple, d'utiliser la législation sur les marques pour entraver l'exercice de la liberté d'opinion ou d'expression des consommateurs ou des salariés à l'égard de la politique ou des pratiques d'une entreprise et de ses produits ou services. Le droit des brevets et des marques semble rencontrer des limites et des problèmes d'application face au développement des réseaux, qui demandent en conséquence un droit protecteur spécifique encore insuffisamment élaboré.

(1) Voir les avis du CES sur les «Réseaux de communications électroniques» (JO C 123 du 25.4.2001, p. 50), sur le «Commerce électronique» (JO C 169 du 16.6.1999, p. 36) et sur les «Incidences du commerce électronique sur le Marché unique» (JO C 123 du 25.4.2001, p. 1).

(2) Avis du CES: JO C 117 du 26.4.2000, p. 1.

(3) «General public licence», licence publique générale qui reconnaît la propriété intellectuelle de l'auteur d'un logiciel gratuit.

3.1.16. En outre, prenant en considération le fait que les tentatives d'interception et de prise de contrôle ou de vol de données sensibles s'effectuent principalement contre des réseaux militaires, administratifs et ceux des entreprises, le Comité appelle les institutions européennes et tous les États membres à lutter conjointement contre toutes les interceptions et tentatives de pénétration à des fins d'espionnage militaire ou industriel et commercial, allant ainsi contre les intérêts stratégiques et économiques de l'Europe.

3.1.17. Les mesures de sécurité, la surveillance des accès, les règles et protocoles internes, les redondances matérielles (machines à tolérance de panne, sites miroirs et proxy, sauvegardes fréquentes et délocalisées de données) exigent des moyens logiciels et matériels, une veille et une mise à jour permanentes par des personnes très qualifiées, et ont en conséquence un coût important tandis que, tant en raison d'une insuffisance d'information technique et de prise de conscience que de leurs possibilités financières, en particulier s'agissant des PME-PMI, elles posent des problèmes importants de mise en œuvre aux entreprises publiques et privées et aux administrations. Les équipes d'alerte d'urgence devraient être bien équipées et prendre en considération les besoins des PME-PMI.

3.2. Observations particulières

3.2.1. Observations particulières sur les risques et moyens de lutte envisagés

3.2.1.1. Protection de la vie privée et lutte contre la cybercriminalité et l'espionnage

3.2.1.1.1. Le Comité partage pleinement la priorité accordée par la Commission à la protection de la vie privée et de la confidentialité des données individuelles dans la politique qu'elle propose. La protection des droits fondamentaux et de la liberté d'information et de communication doivent constituer le cœur de toute stratégie en matière de protection des données et des communications, de même que la protection des intérêts collectifs, à commencer par la nécessité d'assurer la sécurité nationale et le fonctionnement normal des institutions démocratiques et des administrations publiques. Il partage l'idée qu'il faut développer et adapter les moyens destinés à ces fins, qu'ils relèvent de la législation, de la coopération, de la recherche ou de la normalisation.

3.2.1.1.2. Si la possibilité d'interception légale dans le respect des procédures judiciaires appropriées doit être maintenue, les moyens de chiffrement «fort» peuvent rendre impossible le décryptage des messages. La grande criminalité utilise les moyens les plus modernes et les plus sûrs pour protéger ses

communications. Une coopération juridique et technologique doit en conséquence être développée au plan européen international contre la grande criminalité et le terrorisme, comme le Comité l'a souligné notamment dans ses avis sur la lutte contre le blanchiment de capitaux et contre la cybercriminalité ⁽¹⁾.

3.2.1.1.3. Il est également indispensable, dans le cadre de la politique de concurrence, de surveiller les processus de concentration et de monopolisation en ce qui concerne les contenus (information, culture, ...), et les différents segments des «tuyaux» de l'internet. La Commission devrait aussi veiller à l'établissement d'un «gouvernement» du réseau plus représentatif des 370 millions d'utilisateurs actuels, réellement transparent, car l'actuel «gouvernement» multicéphale reste concentré en Amérique du Nord et sous contrôle étroit du Département du Commerce des États-Unis, en particulier pour l'attribution de la gestion des noms de domaines et le choix des registrars ⁽²⁾.

3.2.1.1.4. Les opérateurs doivent garantir effectivement, pour protéger le droit à la vie privée et à la confidentialité de leurs clients, l'utilisation des moyens de surveillance matérielle de leurs installations et de chiffrement des communications les plus en rapport avec l'importance des droits à protéger, en fonction de l'évolution des techniques. Ils y sont d'ailleurs tenus entre autres par la directive 97/66/CE ⁽³⁾.

3.2.1.1.5. Les utilisateurs de leur côté, doivent pouvoir chiffrer de manière suffisamment sûre les données sensibles qu'ils peuvent être amenés à transmettre sur le réseau, mais sont généralement peu au fait des moyens appropriés et de la façon de les mettre en œuvre. Pour faire face aux besoins croissants de chiffrement et de sécurité, il sera indispensable de former des spécialistes en nombre suffisant.

3.2.1.1.6. Les intrusions dans les ordinateurs et les réseaux, quelles qu'en soient les motivations (défi intellectuel, vengeance personnelle ou désir de nuire, vol de renseignements ou prise de contrôle à diverses fins) et la dissémination de virus informatiques mettent en péril les droits et intérêts des utilisateurs ainsi que l'intégrité des données, de l'information et des réseaux.

⁽¹⁾ Avis du CES en cours d'élaboration sur un programme sur la protection de l'enfance sur Internet. Voir les avis du CES sur les «Réseaux de communications électroniques» (JO C 123 du 25.4.2001, p. 50), sur le «Commerce électronique» (JO C 169 du 16.6.2001, p. 36) et sur les «Incidences du commerce électronique sur le Marché unique» (JO C 123 du 25.4.2001).

⁽²⁾ Entreprises chargées de l'attribution et de la gestion de certains des noms de premier niveau.

⁽³⁾ Directive sur la protection des données dans le secteur des télécommunications (JO L 24 du 30.1.1998).

3.2.1.1.7. Tout en étant pleinement d'accord avec la Commission sur l'importance des dommages que peuvent causer les diverses formes d'intrusion, allant parfois jusqu'à la prise de contrôle furtive du système, le Comité considère qu'il serait cependant excessif d'assimiler les hackers mettant seulement en évidence des failles de sécurité sans intention criminelle — ce qui peut permettre de les corriger — à ceux qui s'introduisent dans les systèmes à de telles fins (crackers), et la législation pénale que la Commission pourra proposer devra rester proportionnée aux crimes et délits éventuels, qui doivent rester précisément définis et qualifiés, et prendre en considération l'intention des auteurs d'intrusions.

3.2.1.2. Droit communautaire applicable et technologies disponibles

3.2.1.2.1. Le droit communautaire requiert que les États membres prennent toutes les mesures nécessaires pour assurer la disponibilité des réseaux publics en cas de coupure du réseau due à une catastrophe naturelle [Directive Interconnexion 97/33/CE⁽¹⁾ et Directive Téléphonie vocale 98/10/CE⁽²⁾], mais le Comité suggère à la Commission de faire procéder à une étude comparative des mesures prises et de leur effectivité dans tous les États membres.

3.2.1.2.2. Les déclarations mensongères faites par des personnes physiques ou morales peuvent causer des dommages et pour toute transaction importante, il est nécessaire d'authentifier les personnes et de s'assurer de la véracité des déclarations.

3.2.1.2.3. Les protocoles SSL et IPsec permettent de communiquer sur l'internet et les canaux ouverts avec un certain niveau de sécurité, mais qui n'offre pas une garantie suffisante. Dans la directive sur les signatures électroniques⁽³⁾, il est prévu qu'un tiers, le «prestataire de service de certification», puisse offrir une telle garantie.

3.2.1.2.4. L'adoption de cette solution est confrontée au même problème que le chiffrement — le besoin d'interopérabilité et de gestion des clés. Dans un VPN (réseau virtuel privé), il est possible de recourir à des solutions propriétaires. Par contre, il s'agit d'un obstacle majeur pour les réseaux publics.

3.2.1.2.5. Pour ces raisons, la directive sur les signatures électroniques constitue la base juridique et l'instrument essentiel pour faciliter l'authentification électronique dans l'UE.

3.2.1.3. Nouveaux défis, nouveaux risques et analyse coûts-bénéfices

3.2.1.3.1. Le Comité partage l'analyse des nouveaux défis et des nouveaux risques, liés au développement rapide des technologies, à la multiplication et à la diversification des terminaux d'accès, ainsi que les dangers accrus de piratage avec la généralisation des terminaux connectés en continu, avec une adresse fixe. Il soutient l'approche qui veut concilier sécurité et libertés, protection des réseaux et protection de la vie privée et de la confidentialité.

3.2.1.3.2. En outre, si les moyens de chiffrement plus sûrs ont demandé une évolution des législations, pour permettre un «cryptage fort», celle-ci a été parfois très tardive en raison de considérations de sécurité; mais la dissimulation des messages dans le «bruit» des fichiers d'images ou de sons (stéganographie) offrait déjà le moyen de dissimuler le fait même de l'envoi d'un message chiffré pour les personnes désirant détourner la loi sans être détectées.

3.2.1.3.3. Plusieurs algorithmes sont utilisés, et d'autres plus sophistiqués deviennent disponibles: cela pose de sérieux problèmes de gestion des messages chiffrés selon différentes méthodes par différents correspondants. Même la recommandation d'un système européen, si elle peut faciliter les communications sur le marché intérieur, se heurtera à la diversité des systèmes en cours dans le reste du monde. Cela pèse sur le coût de la sécurité et de sa gestion, même si certains systèmes efficaces sont dans le domaine public et gratuits.

3.2.1.3.4. Néanmoins, le coût de la non-sécurité, alors que des données de plus en plus sensibles circulent, est encore plus élevé. La sécurité sera aussi dans une certaine mesure de plus en plus intégrée aux produits.

3.2.1.3.5. Le Comité considère positivement l'approche européenne proposée par la Commission, tout en étant conscient de ses limites, ainsi que la nécessité d'une action publique, pour suppléer aux carences actuelles du marché et en raison de l'importance des enjeux.

3.2.1.3.6. Il existe déjà des garanties juridiques dans les directives de l'UE sur la protection des données et dans le cadre réglementaire pour les télécommunications. Toutefois, ces mesures doivent être mises en œuvre dans un environnement en évolution rapide, qu'il s'agisse des technologies, de la concurrence, de la convergence des réseaux et de la mondialisation, alors que le marché aura tendance à ne pas investir suffisamment dans la sécurité pour les raisons justement décrites par la Commission, bien que le marché de la sécurité soit en expansion rapide dans le monde.

(1) JO L 199 du 26.7.1997.

(2) JO L 101 du 1.4.1998.

(3) Directive 1999/93/CE, du 13 décembre 1999, sur un cadre commun pour les signatures électroniques, JO L 13 du 19.1.2000, p. 12.

3.2.1.3.7. Il est vrai comme le soutient la Commission que le marché de la sécurité est encore imparfait. L'investissement dans la sécurité n'est rentable que si un nombre suffisant de personnes adopte la même démarche. La recherche de solutions doit donc passer par la coopération. Dans la mesure où une multitude de produits et de services continuent à utiliser des solutions propriétaires, il faut encourager la recherche dans des standards plus généralement admis et plus sûrs et dans l'interopérabilité des systèmes de sécurité. Il vaut mieux, pour le Comité, encourager l'établissement de «common criteria» au niveau international plutôt que des systèmes de certification-authentification qui peuvent pénaliser le consommateur final.

3.2.1.3.8. Premièrement, les dispositions juridiques existantes au niveau de l'UE doivent être mises en œuvre de manière efficace. Le cadre juridique doit rester pertinent et efficace, et sera donc inévitablement amené à évoluer en permanence.

3.2.1.3.9. Deuxièmement, si les forces du marché ne permettent pas actuellement de générer un niveau d'investissement suffisant dans les technologies et la pratique de la sécurité, les mesures politiques proposées par la Commission sont à même de renforcer le processus du marché, qui a d'ailleurs commencé à évoluer.

3.2.1.3.10. Enfin, les services de communication et l'information sont transfrontières. C'est pourquoi une approche politique européenne est requise pour assurer le marché intérieur pour ces services, pour bénéficier de solutions communes et enfin pour agir de manière plus efficace au niveau mondial.

3.2.1.3.11. Le Comité est d'accord avec l'idée que les investissements dans une meilleure sécurité des réseaux engendrent des coûts et des bénéfices sociaux qui ne sont pas correctement reflétés dans les prix du marché. En ce qui concerne les coûts, les acteurs du marché ne sont pas actuellement tenus d'assumer toutes les responsabilités résultant de leur comportement en matière de sécurité; le Comité estime que cette situation ne peut plus durer.

3.2.1.3.12. Le Comité partage aussi l'analyse selon laquelle les bénéfices de la sécurité ne se répercutent pas non plus entièrement sur les prix du marché, bien que les investissements dans ce domaine des opérateurs, des fournisseurs ou des prestataires de services bénéficient non seulement à leurs clients mais en fait à l'ensemble de l'économie et à la sécurité générale des communications.

3.2.1.3.13. Il partage également l'idée que les utilisateurs ne sont pas conscients de tous les risques de sécurité tandis qu'un grand nombre d'opérateurs, de vendeurs ou de fournisseurs de services ont du mal à évaluer l'existence et l'ampleur des

vulnérabilités. De même, de nombreux services, applications et logiciels nouveaux offrent des caractéristiques attrayantes, mais celles-ci peuvent constituer une source de nouvelles vulnérabilités. Il conviendrait de tester plus à fond les produits avant leur mise sur le marché.

3.2.2. Observations particulières sur le cadre politique européen proposé

3.2.2.1. Le Comité est conscient de la vulnérabilité intrinsèque du réseau mondial, en particulier au niveau du routage des paquets de données, et du fait que la masse toujours croissante des données en circulation ne permet pas d'envisager sa sécurisation générale par filtrage, en dehors des terminaux. Il appuie en général les propositions d'action contenues dans le cadre politique proposé.

3.2.3. Sensibilisation

3.2.3.1. Les propositions faites sont judicieuses pour sensibiliser toutes les personnes et organisations concernées. La sécurisation des terminaux et des communications dépend principalement de la conscientisation et de l'action informée des usagers eux-mêmes.

3.2.4. Système européen d'information rapide

3.2.4.1. Le Comité soutient la proposition d'un système européen d'alerte et d'information rapide indiquant les problèmes et les solutions à appliquer et les autres propositions de la Commission en matière d'analyse, de détection précoce, de diffusion d'informations et de conseils et de coopération européenne et mondiale, tout en développant des infrastructures adaptées dans l'ensemble de l'Union et leur coopération permanente effective.

3.2.4.2. Néanmoins, en ce qui concerne les rapports que devraient faire les entreprises mais aussi, selon le Comité, les administrations et autres organismes, celui-ci comprend que le caractère confidentiel du mécanisme de compte rendu des attaques favorisera le retour d'informations, mais il rappelle qu'il y a toujours des fuites ou des révélations publiques faites par les hackers, et la connaissance assez rapide de la nature des attaques et failles et surtout des mesures prises pour y remédier constituerait plutôt un facteur de confiance du public.

3.2.4.3. Les systèmes de détection et d'alerte devraient aussi, selon le Comité, concerner la découverte de failles dans les logiciels commerciaux ou gratuits, ainsi que tout facteur technologique ou autre pouvant ouvrir la porte à d'éventuelles attaques. Le système d'analyse précoce pourrait assumer cette fonction, ainsi qu'une veille technologique et également un suivi des sites de hackers et de pirates et de diverses publications underground traitant des méthodes utilisables voire publiant des programmes «clés en mains» de création de virus ou d'intrusion, dont se servent les script kiddies (1).

3.2.5. Soutien technologique

3.2.5.1. Le Comité approuve le soutien envisagé aux efforts de recherche. Il tient cependant à rappeler que la cryptographie constitue une science maîtrisée tout au plus par quelques dizaines d'experts dans le monde; un grand nombre travaille pour la NSA (2). Comment retenir les experts européens avec lesquels développer la recherche ? Quels sont les moyens effectifs en Europe ? La NSA a 10 ou 15 ans d'avance et dispose de moyens de calcul (et de décryptage) qu'il paraît difficile d'égaliser rapidement. Quels moyens concrets — et nécessairement importants — seront-ils mis au service de la recherche (3) ?

3.2.5.2. Une politique d'intégration des hackers et des experts «informels» existants pourrait constituer une piste complémentaire, au lieu de l'attitude de rejet dans la marginalisation ou une pénalisation excessive par confusion avec des actes très graves, qui semble se développer en Europe envers des personnes ne causant aucun dommage direct à autrui ou à la société. Il faudrait, tout en assurant la pénalisation dissuasive des actes de piraterie ou de terrorisme sur les réseaux, ne pas assimiler systématiquement à ces actes les recherches de failles de sécurité effectuées dans un but d'information des auteurs de logiciels ou des gestionnaires de réseaux afin qu'ils renforcent leurs protections, dans la mesure où cette recherche des failles de sécurité n'est pas effectuée à des fins nuisibles, telles que le sabotage, le détournement de données confidentielles, l'utilisation secrète du réseau, l'enrichissement personnel ou la diffusion de virus informatiques.

3.2.5.3. La mise dans le public des découvertes sans que les intéressés directs soient informés bien longtemps à l'avance et sans leur accord constitue cependant un acte répréhensible pouvant faire l'objet d'une incrimination délictuelle proportionnée. Mais pour les personnes ne commettant pas de crime ni de délit grave ou ne causant pas de dommages pécuniaires, il conviendrait de s'efforcer de les insérer dans le cadre de la légalité et de mettre à profit leurs compétences au bénéfice de la société. Ainsi, ces compétences rares ne pourraient pas être exposées à un risque de détournement ou d'utilisation par des criminels ou des terroristes, si elles restaient marginalisées et étaient criminalisées.

3.2.6. Soutien à une normalisation et une certification orientées vers les besoins du marché

3.2.6.1. Le Comité partage l'analyse de la Commission sur le trop grand nombre de normes et de systèmes en concurrence, qui constituent des obstacles à la sécurité et aux progrès de la signature et des moyens de paiement électroniques sécurisés, et souligne le besoin de normes communes, de critères communs permettant d'éviter les rigidités dans le marché et d'interopérabilité.

3.2.6.2. Il appuie les actions proposées, mais en souligne certaines difficultés, liées à la nature privée et insuffisamment représentative du «gouvernement» actuel de l'internet, qui définit notamment les normes. Il s'agira d'un travail de longue haleine, qui demandera patience et coopération.

3.2.7. Cadre juridique

3.2.7.1. Le Comité approuve le projet de spécification pour les réseaux et l'internet du cadre législatif existant en matière de télécommunications et de protection des données.

3.2.7.2. Les actions proposées sont judicieuses et le Comité approuve les initiatives envisagées pour parvenir à un droit pénal harmonisé et pour renforcer la coopération pénale entre les États membres contre la cybercriminalité, sans remettre en cause la libéralisation du commerce des outils de chiffrement fort, seuls susceptibles d'assurer une sécurité efficace. La coopération en matière civile et commerciale joue également un rôle important dans la lutte contre les cybercriminels (circuits financiers, fraude fiscale, etc.).

(1) Jeunes apprentis pirates sans qualifications techniques, qui se contentent de copier ce qu'ils trouvent dans les sites et publications underground.

(2) National Security Agency, l'Agence de Sécurité Nationale des États-Unis.

(3) Avis du CES sur le 6^e Programme-cadre RDT (JO C 260, du 17.9.2001, p. 3).

3.2.7.3. Cependant, la question de la coopération pénale devrait, selon le Comité, s'étendre au plan global, et la stratégie européenne en ce domaine devrait faire l'objet d'une ligne d'action dans le cadre politique proposé. Le Comité note avec plaisir qu'une proposition formelle de la Commission à ce sujet est attendue dans les prochaines semaines.

3.2.8. Sécurité dans les administrations publiques

3.2.8.1. Le Comité approuve les actions envisagées, compte tenu du caractère personnel d'un nombre important de données traitées par les administrations publiques, et aussi du fait que leurs sites peuvent faire l'objet d'attaques de type terroriste ou pour des raisons de politique intérieure ou extérieure de l'État, comme l'ont montré Code Red (un virus polymorphe) ou Nimda récemment. La Commission devrait retenir ces derniers motifs d'attaques comme une raison supplémentaire de toujours mieux sécuriser ses sites et réseaux officiels et ceux des États membres.

3.2.9. Coopération internationale

3.2.9.1. Il s'agit, aux yeux du Comité, d'un chapitre essentiel mais délicat et difficile de la politique européenne de sécurité des réseaux et des communications, qui pose de sérieux problèmes de solidarité interne, et de politique extérieure et de sécurité commune, ainsi que de gouvernance des réseaux interconnectés et de l'internet.

3.2.9.2. La proposition d'action dans ce domaine, consistant à poursuivre et développer la coopération dans les différentes instances internationales sur la fiabilité des réseaux, est diplomatiquement formulée en termes anodins.

3.2.9.3. Pourtant, le Comité estime qu'il conviendrait également de poursuivre le débat dans les instances internationales appropriées et dans le dialogue transatlantique sur les questions de sécurisation, d'interopérabilité des clés et systèmes de chiffrement, des problèmes de faiblesses éventuelles de certains standards qui pourraient être connus mais non divulgués par une partie. Il serait également souhaitable de coopérer étroitement en matière de circulation internationale des données personnelles, de coopération pénale et civile contre la cybercriminalité, c'est-à-dire de la sécurisation effective et de la gestion transparente et équilibrée du réseau mondial, dont l'importance stratégique est désormais reconnue comme essentielle pour la vie et le bien-être de nos sociétés. L'OCDE, qui travaille sur les questions de sécurité des réseaux, constitue une

des instances pertinentes de coopération internationale à ce sujet. Il est urgent d'aboutir à des résultats pratiques à un niveau global.

3.2.9.4. Le Comité appuie et considère comme très importante la proposition de la Commission de constituer, au niveau européen, un forum réunissant tous les acteurs concernés pour débattre de l'ensemble des problèmes et proposer des solutions aux institutions.

4. Conclusions

4.1. Des solutions logicielles et matérielles, en évolution constante, existent et sont assez efficaces, telles que celles décrites dans la communication; en outre l'intégrité d'un fichier peut aussi être garantie par l'usage d'un algorithme d'empreinte numérique, et l'empreinte, unique, indique que le fichier transmis n'a pas subi de modifications.

4.2. Mais ce sont, aux yeux du Comité, la sensibilisation des usagers, l'information et la formation, qui constituent la clé de toute stratégie de sécurité, car sans elles, les moyens et solutions disponibles ne seront pas correctement utilisés; elles renforcent aussi la confiance dans la fiabilité globale du système si toutes les précautions élémentaires sont prises régulièrement par tous et si les entreprises investissent au niveau requis dans la sécurisation de leurs systèmes.

4.3. Mais le coût de la sécurité est très élevé, et le manque d'interopérabilité des solutions constitue un obstacle important, auquel l'open source pourrait apporter une contribution en stimulant la concurrence et l'émulation.

4.4. Ces problèmes, s'ils ne sont pas rapidement résolus dans le cadre européen et international — et l'Europe doit prendre une place effective dans le «gouvernement» de l'Internet — vont continuer de peser sur le développement de l'e-Europe, du commerce électronique et sur la gestion des entreprises, des services publics et des administrations.

4.5. Il est en tout état de cause indispensable pour la sécurité des réseaux, d'obtenir l'application généralisée de mesures de protection et de défense efficaces et proportionnées, qu'il s'agisse de solutions logicielles pour les particuliers (antivirus mis à jour régulièrement) ou de solutions combinées et plus ou moins lourdes pour les autres usagers (pare-feu, surveillance des ports de communication externe, séparation [DMZ ⁽¹⁾], boucliers, et autres techniques, logiciels et matériels pertinents).

(¹) DMZ: DeMilitarized Zone, zone «démilitarisée», sorte de zone tampon isolant le réseau interne.

4.6. Une dissuasion par des sanctions pénales appropriées relève de la responsabilité des États membres, mais le Comité estime qu'il revient à la Commission de proposer un cadre global unificateur pour l'approche pénale communautaire et pour la coopération judiciaire internationale.

4.7. La mise sur le marché de certains produits qui peuvent comporter des backdoors⁽¹⁾ intentionnelles, qui mettront parfois des années à être décelées, doit être prise en considération, et devrait faire l'objet de sanctions, de même que les «espioniciels» (spyware) souvent présents dans les logiciels de démonstration, certains logiciels gratuits et certains systèmes d'enregistrement des licences en ligne.

4.8. Même les failles qui pourraient être non intentionnelles prennent du temps à être mises à jour, et peuvent être utilisées comme backdoors par des personnes informées.

(1) Portes d'accès cachées.

4.9. Des autorités nationales ad hoc, indépendantes, impartiales, représentatives, qu'il s'agisse d'organes existant dont il faudrait étendre la mission ou d'organes à créer là où ils n'existeraient pas encore (pays candidats, qu'il faudrait associer), devraient suivre ces problèmes de sécurité pour contribuer à formuler des recommandations et des standards et protéger les droits fondamentaux. En effet, des projets de législations en préparation demanderaient un examen plus attentif, afin de concilier les impératifs de la lutte antiterroriste avec les principes de liberté individuelle qui doivent être préservés.

4.10. Pour le CES l'Internet doit, en tout état de cause, rester flexible et facile d'accès, et continuer à offrir un espace de liberté d'information et de communication dans une société ouverte et démocratique, tout en étant plus sûr pour les divers utilisateurs, dans la diversité des usages légaux des réseaux et de l'Internet et de leur expansion.

Bruxelles, le 28 novembre 2001.

Le Président
du Comité économique et social
Göke FRERICHS