COMMISSION EUROPÉENNE

Bruxelles, le 30.9.2010
SEC(2010) 1123 final

DOCUMENT DE TRAVAIL DES SERVICES DE LA COMMISSION

RÉSUMÉ DE L'ANALYSE D'IMPACT

accompagnant la

Proposition de

DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL

relative aux attaques visant les systèmes d'information et abrogeant la décision-cadre 2005/222/JAI

{COM(2010) 517 final}
{SEC(2010) 1122 final}

RÉSUMÉ DE L'ANALYSE D'IMPACT

1. DEFINITION DU PROBLEME

Tout d'abord, le nombre d'attaques contre des systèmes d'information a considérablement augmenté depuis l'adoption de la décision-cadre relative aux attaques visant les systèmes d'information («décision-cadre relative aux attaques»). Selon l'une des principales sociétés spécialisées dans la sécurité sur l'internet, le nombre de menaces dirigées contre les informations confidentielles (par opposition aux informations accessibles au public) s'est sensiblement accru en 2008, passant de 624 267 à 1 656 228 nouvelles menaces pour cette même année[1]. En outre, on a observé plusieurs attaques d'une ampleur et d'une dangerosité jusque-là inégalées, comme celles lancées en Estonie en 2007 et en Lituanie en 2008. En mars 2009, les systèmes informatiques d'organisations des secteurs public et privé de 103 pays ont été attaqués par un réseau d'ordinateurs compromis qui extrayaient des documents sensibles et classifiées[2], au moyen de «réseaux zombies»[3], c'est-à-dire des réseaux d'ordinateurs contaminés qui peuvent être contrôlés à distance. Enfin, un réseau zombie appelé «Conficker» (aussi connu sous le nom de «Downup», «Downadup» et «Kido») se propage actuellement dans le monde; il se répand et intervient à une échelle et avec une ampleur sans précédent depuis novembre 2008, touchant des millions d'ordinateurs de par le monde[4].

Ensuite, il est difficile d'opposer une réponse coordonnée et efficace à ces attaques en l'absence d'une coopération suffisante entre les États membres, et en particulier entre les forces de l'ordre et les autorités judiciaires au sein de l'UE. Bien que, selon le rapport sur la transposition de la décision-cadre relative aux attaques, une majorité d'États membres ait mis en place des points de contact permanents ainsi que le requiert son article 11, la réactivité et la capacité de ces derniers à répondre à des demandes urgentes de coopération continuent de poser problème[5].

En effet, l'existence d'un point de contact ne garantit pas son bon fonctionnement. Dans leurs notifications à la Commission, plusieurs États membres signalaient que, si leurs points de contact respectifs étaient certes en place, ils ne fonctionnaient pas vingt-quatre heures sur vingt-quatre comme le requiert la décision-cadre relative aux attaques. Ils ne peuvent donc pas répondre à des demandes urgentes en dehors des heures de bureau. Le manque d'efficacité

---

1 http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf, p.10.

2 ww.theglobeandmail.com/servlet/story/RTGAM.20090328.wspy0328/BNStory/International/home?cid=al_gam_mostemail

3 Un réseau zombie est un réseau d'ordinateurs contaminés par un logiciel malveillant (virus informatique). Un tel réseau d'ordinateurs compromis («zombies») peut être activé pour exécuter certaines actions, comme attaquer des systèmes d'information (cyberattaques). Les «zombies» peuvent être contrôlés, souvent à l'insu des utilisateurs de ces ordinateurs, par un autre ordinateur, également appelé «centre de commande et de contrôle». Les personnes qui gèrent ce centre font partie des auteurs de l'infraction puisqu'elles utilisent les ordinateurs compromis pour attaquer des systèmes informatiques. Il est très difficile de repérer les coupables car les ordinateurs qui composent le réseau zombie et lancent l'attaque peuvent se trouver ailleurs.

4 http://www.lemonde.fr/technologies/article/2009/03/31/virus-conficker-catastrophe-ou-poisson-d-avril_1174916_651865.html

5 Rapport de la Commission au Conseil fondé sur l'article 12 de la décision-cadre du Conseil du 24 février 2005 relative aux attaques visant les systèmes d'information, COM(2008)0448 final.

des points de contact ou leur incapacité à satisfaire les demandes de coopération du secteur privé fait souvent obstacle à la coopération entre les secteurs public et privé.

Enfin, on ne dispose encore que de peu de données sur les cyberattaques, ainsi que sur les enquêtes policières et poursuites judiciaires auxquelles elles donnent éventuellement lieu. Tous les États membres ne collectent pas des données sur les cyberattaques. Ceux qui le font appliquent un procédé qui ne permet pas la comparaison des données, du fait de la divergence des méthodes statistiques utilisées.

Les victimes des attaques à grande échelle ciblant les systèmes d'information sont essentiellement les particuliers qui utilisent les systèmes d'information, ainsi que les pouvoirs publics centraux et locaux, les organisations internationales et le secteur privé.

Les attaques peuvent être lancées à partir de pays tiers contre des cibles situées sur le territoire de l'UE, ou inversement.

2. SUBSIDIARITE

La cybercriminalité est un problème véritablement international, contre lequel on ne peut que rarement lutter dans un contexte purement national. La nécessité de mener des actions internationales et à l'échelle de l'Union pour prévenir et endiguer ce problème est largement admise. En effet, la plupart des attaques ignorent les frontières de l'UE. Elles touchent tous les États membres, et il est manifeste que nombreuses sont celles qui impliquent des activités d'un État membre à l'autre. Les systèmes d'information sont souvent techniquement interconnectés et interdépendants au-delà des frontières. Les experts s'accordent donc à dire que des actions au niveau international et à l'échelle de l'Union s'imposent et que les États membres ne peuvent à eux seuls réaliser de manière suffisante l'objectif de lutter efficacement contre cette criminalité.

Si elle se limite au niveau national, la lutte contre la cybercriminalité risque d'engendrer fragmentation et inefficacité à travers l'Europe. Les différences entre les stratégies nationales et l'absence de coopération transfrontières systématique réduisent considérablement l'efficacité des contre-mesures nationales, en partie à cause de l'interconnectivité des systèmes d'information, car un déficit de sécurité dans un pays peut accroître la vulnérabilité d'autres pays.

3. QUELS SONT LES OBJECTIFS?

3.1 Objectifs généraux, spécifiques et opérationnels

L'action de l'UE a pour objectif général de réprimer et de poursuivre la criminalité, organisée ou non, conformément à l'article 67 du traité sur le fonctionnement de l'Union européenne, en luttant contre les cyberattaques à grande échelle visant les systèmes d'information.

A Objectif spécifique: Poursuivre et condamner les auteurs d'attaques à grande échelle grâce au rapprochement des règles pénales applicables aux attaques contre les systèmes d'information

B Objectif spécifique: Améliorer la coopération transfrontières entre les forces de l'ordre

C Objectif spécifique: Instaurer des dispositifs de suivi et une collecte des données efficaces

4. QUELLES SONT LES OPTIONS D'ACTION?

4.1 Option (1): Statu quo / Pas de nouvelle action de l'UE

Cette option implique que l'UE ne prenne aucune initiative supplémentaire pour lutter contre ce type particulier d'infraction informatique. Les actions en cours, en particulier les programmes destinés à renforcer la protection des infrastructures d'information critiques et à améliorer la coopération public-privé contre la cybercriminalité, se poursuivraient.

4.2 Option (2): Élaboration d'un programme intensifiant les efforts de lutte contre les attaques visant les systèmes d'information par des mesures non législatives

Parallèlement au programme de protection des infrastructures d'information critiques, des mesures non législatives seraient axées sur la répression transfrontières et la coopération public-privé et devraient faciliter la poursuite de l'action coordonnée au niveau de l'Union. Une proposition non législative pourrait inclure des actions telles que la consolidation de l'actuel réseau 24/7 de points de contacts des forces de l'ordre; la mise en place d'un réseau européen de points de contact public-privé réunissant les experts en cybercriminalité et les forces de l'ordre; ainsi que l'élaboration d'un modèle d'accord européen sur les niveaux de service pour la coopération policière avec des opérateurs du secteur privé.

4.3 Option (3): Mise à jour sélective de la décision-cadre sur les attaques pour répondre à la menace spécifique d'attaques à grande échelle contre des systèmes d'information

Cette option suppose l'introduction d'une législation spécifique ciblée (c'est-à-dire limitée) visant à lutter contre les attaques à grande échelle, particulièrement dangereuses, ciblant des systèmes d'information. Cette législation ciblée serait associée à des mesures destinées à intensifier la coopération opérationnelle transfrontières pour lutter contre les attaques visant des systèmes d'information et tendrait à accroître les sanctions minimales déjà prévues. Cette option prendrait la forme d'une mise à jour de la décision-cadre en vigueur, qui serait complétée par plusieurs mesures non législatives, telles que l'amélioration de la préparation, la sécurité et la résilience des infrastructures d'information critiques, la protection de celles-ci, le renforcement d'instruments et de procédures régissant la coopération transfrontières des forces de l'ordre, et l'échange de bonnes pratiques.

4.4 Option (4): Adoption d'un corpus complet de législation européenne contre la cybercriminalité

Constatation étant faite de la nécessité de réagir rapidement à la multiplication d'attaques sophistiquées contre des systèmes d'information, il pourrait être opportun de mettre également en place une législation européenne plus large sur la cybercriminalité en général. Cette législation couvrirait non seulement les attaques contre les systèmes d'information, mais aussi des questions telles que la cyberdélinquance financière, la diffusion de contenus illégaux sur l'internet, les collectes/stockages/transferts de preuves électroniques et la formulation règles de compétence plus détaillées. Cette législation européenne serait applicable parallèlement à la convention du Conseil de l'Europe sur la cybercriminalité, qui serait notamment complétée par de nouvelles dispositions jugées nécessaires au sein de l'UE.

4.5 Option (5): Mise à jour de la convention du Conseil de l'Europe sur la cybercriminalité

Cette option obligerait à renégocier une bonne partie de la convention actuelle, ce qui prendrait du temps et ne serait donc pas compatible avec le calendrier d'action proposé dans l'analyse d'impact. Il ne semble d'ailleurs pas y avoir de volonté internationale de renégocier la convention. L'actualisation de cette dernière ne peut donc être considérée comme une option réalisable puisqu'elle dépasserait le délai d'action prescrit.

5. ANALYSE D'IMPACT

Options	Impact économique	Impact social	Impact sur les droits fondamentaux	Impact sur les pays tiers	Pertinence pour les objectifs A, B, C	Cohérence avec le droit international
Option 1 Statu quo / Pas de nouvelle action de l'UE	0	0	0	-	0	0
Option 2: Élaboration d'un programme intensifiant les efforts de lutte contre les attaques visant les systèmes d'information par des mesures non législatives	-/+	++	-/+	++	A + B ++ C +	-/+
Option 3: Mise à jour sélective de la décision-cadre sur les attaques pour répondre à la menace spécifique d'attaques à grande échelle contre les systèmes d'information	--/++	-/+++	-/++	+++	A +++ B +++ C +++	++
Option 4: Adoption d'un corpus complet de législation européenne sur la cybercriminalité.	---/+++	+++	--/++	++	A ++ B ++ C ++	-/++
Option privilégiée (options 2 et 3) Combinaison entre des mesures non législatives et une mise à jour sélective de la décision-cadre sur les attaques	--/+++	+++	-/++	+++	A +++ B +++ C +++	++

6. QUE RESSORT-IL DE LA COMPARAISON DES DIFFERENTES OPTIONS?

6.1 Option (1) - Statu quo

Cette option rendra inévitablement plus vulnérable la position des acteurs privés, des États membres et de l'Union dans son ensemble dans leur lutte contre la cybercriminalité, en raison de la nature et de la croissance de celle-ci. Même si le niveau des actions actuellement menées se maintient, il serait nécessaire de veiller à la coordination à l'échelle européenne.

6.2 Option (2): Élaboration d'un programme intensifiant les efforts de lutte contre les attaques visant les systèmes d'information par des mesures non législatives

Cette option présente tous les avantages et les inconvénients d'un instrument non contraignant. Elle a pour effet positif de permettre de décrire chaque option d'une manière qui soit cohérente avec les meilleures pratiques nationales, facilitant ainsi la détermination des mesures les plus efficaces.

En revanche, cette option ne permet pas de réaliser aussi efficacement les objectifs fixés.

6.3 Option (3): Mise à jour sélective de la décision-cadre sur les attaques pour répondre à la menace d'attaques à grande échelle contre des systèmes d'information

Cette option permet de répondre de façon opportune et sélective aux problèmes décelés. Elle aborde les questions de droit pénal à prendre en compte pour poursuivre efficacement les auteurs de ces infractions. Elle tend aussi à améliorer la coopération internationale par la mise en place d'un mécanisme d'aide internationale immédiate en cas de demandes urgentes de coopération et encourage la coopération avec le secteur privé au moyen de mesures d'accompagnement, telles que les réunions d'experts. Cette option établit aussi plusieurs circonstances aggravantes, comme les attaques à grande échelle, ainsi que les attaques commises en dissimulant l'identité réelle de l'auteur et en causant un préjudice au propriétaire légitime de l'identité.

Enfin, elle instaure des obligations de suivi pour pouvoir mesurer l'étendue du problème.

6.4 Option (4): Adoption d'un corpus complet de législation européenne contre la cybercriminalité

Tout comme l'option 3, cette option a pour valeur ajoutée d'arrêter des dispositions contraignantes; elle devrait donc assurer une plus grande efficacité si elle est entièrement mise en œuvre. Elle devrait aussi maximiser l'effet positif des instruments tant législatifs que non législatifs sur un ensemble de questions liées à la cybercriminalité, au-delà des seules attaques à grande échelle. En outre, elle aborderait le cadre pénal et améliorerait en même temps la coopération transfrontières des services répressifs. Cependant, à l'heure actuelle, cette approche globale ne recueille pas le consensus des parties prenantes, alors que sa mise en œuvre ferait davantage progresser la lutte contre la cybercriminalité que toutes les autres options.

7. OPTION PRIVILEGIEE

Au terme de l'analyse des incidences économiques, sociales et sur les droits fondamentaux, les options 2 et 3, compte tenu des solutions qu'elles apportent aux problèmes, paraissent les plus susceptibles d'atteindre les objectifs fixés.

D'une manière générale, l'option privilégiée serait une combinaison des options 2 et 3, puisqu'elles sont complémentaires et, partant, correspondent le mieux aux objectifs définis, tant sur le fond que du point de vue du calendrier.

8. SUIVI ET EVALUATION

Il conviendrait de publier un rapport sur la transposition dans un délai de deux ans à compter de la date d'entrée en vigueur de la directive. Ce rapport devra s'intéresser à la transposition correcte de la directive par les États membres.

En outre, il conviendrait d'évaluer régulièrement de quelle façon et dans quelle mesure la directive aura contribué à la réalisation de ses objectifs. La première évaluation devrait avoir lieu dans un délai de cinq ans à compter de l'entrée en vigueur de la directive; par la suite, la Commission publiera tous les cinq ans des rapports d'évaluation, qui contiendront des informations sur la mise en œuvre. À la lumière des conclusions et recommandations des évaluations, la Commission devrait prendre en considération toute modification ultérieure de la directive ou toute autre évolution possible de celle-ci.