Revue québécoise de droit international
Quebec Journal of International Law
Revista quebequense de derecho internacional

La lutte contre la cybercriminalité à l'échelle de l'Union : analyse de l'évolution juridique d'un phénomène à la confluence de plusieurs agendas institutionnels

Pierre Berthelet

Special Issue, November 2018

L'intégration européenne. Soixante ans du *Traité de Rome* : tous les chemins mènent-ils encore à Bruxelles ?

URI: https://id.erudit.org/iderudit/1067257ar
DOI: https://doi.org/10.7202/1067257ar

See table of contents

Publisher(s)

Société québécoise de droit international

ISSN

0828-9999 (print)
2561-6994 (digital)

Explore this journal

Cite this article

Berthelet, P. (2018). La lutte contre la cybercriminalité à l'échelle de l'Union : analyse de l'évolution juridique d'un phénomène à la confluence de plusieurs agendas institutionnels. *Revue québécoise de droit international / Quebec Journal of International Law / Revista quebequense de derecho internacional*, 25–39. https://doi.org/10.7202/1067257ar

Article abstract

The fight against cyber crime in the European Union is based on the idea that its Member States cannot act separately to fight this transnational phenomenon. Then, a specific action has been gradually structured. If the fight against "computer crime" was initially the main topic, the term "cybercrime" will gradually become more and more used by the UE institutions. The fight against this phenomenon tends to be situated at the convergence of various institutional agendas that promote a powerful integrative dynamic: the European digital market, the European criminal area, cybersecurity and internal security in particular.

LA LUTTE CONTRE LA CYBERCRIMINALITÉ À L'ÉCHELLE DE L'UNION : ANALYSE DE L'ÉVOLUTION JURIDIQUE D'UN PHÉNOMÈNE À LA CONFLUENCE DE PLUSIEURS AGENDAS INSTITUTIONNELS

Pierre Berthelet[*]

La lutte contre la cybercriminalité à l'échelle de l'Union européenne naît du constat que, face à un phénomène d'ampleur transnationale, ses États membres ne peuvent agir de manière isolée. Une action spécifique se structure dès lors progressivement. S'il était davantage question de « criminalité informatique », le terme de cybercriminalité va peu à peu s'imposer, au fur et à mesure que l'action de l'Union se singularise. La lutte contre ce phénomène tend à se trouver à la convergence d'agendas institutionnels qui favorisent une dynamique intégrative puissante : le marché numérique européen, l'espace pénal européen, la cybersécurité et la sécurité intérieure, notamment.

The fight against cyber crime in the European Union is based on the idea that its Member States cannot act separately to fight this transnational phenomenon. Then, a specific action has been gradually structured. If the fight against "computer crime" was initially the main topic, the term "cybercrime" will gradually become more and more used by the UE institutions. The fight against this phenomenon tends to be situated at the convergence of various institutional agendas that promote a powerful integrative dynamic: the European digital market, the European criminal area, cybersecurity and internal security in particular.

La lucha contra el delito cibernético en la Unión Europea se basa en la idea de que sus Estados miembros no pueden actuar por separado para luchar contra este fenómeno transnacional. Entonces, una acción específica se ha estructurado gradualmente. Si la lucha contra el "crimen informático" fue inicialmente el tema principal, el término "delito cibernético" se utilizará cada vez más por las instituciones de la UE. La lucha contra este fenómeno tiende a converger en varias agendas institucionales que promueven una poderosa dinámica integradora: el mercado digital europeo, el área criminal europea, la ciberseguridad y la seguridad interna en particular.

[*] Docteur en droit. Chercheur associé CREOGN (Gendarmerie - Melun) /CESICE (Univ. Grenoble) / CERIC (Univ. Marseille/Aix-en-P.).

La lutte menée contre la cybercriminalité est une priorité politique européenne, cette affirmation étant devenue désormais presque une tautologie. Un tel phénomène est en effet source d'inquiétude. La Commission qualifie ce phénomène de menace grave au regard de son caractère « galopant[1] ». La directive de 2013 dite « cyberattaques » constate que « les attaques contre les systèmes d'information, et en particulier celles liées à la criminalité organisée, constituent une menace croissante au sein de l'Union et à l'échelle mondiale[2] ». La stratégie européenne sur la cybersécurité approuvée la même année indique que la cybercriminalité fait plus d'un million de victimes sur la planète quotidiennement et constitue, à ce titre, la forme de criminalité qui croît le plus vite[3]. Celle de 2017 note de son côté une augmentation exponentielle des risques.

Au regard des textes adoptés, l'Union adopte une approche englobante, correspondant à une tendance actuelle abordant la cybercriminalité sous un angle large, de manière à comprendre tout type d'infractions commis au moyen ou à l'encontre d'appareils électroniques, des réseaux informatiques ou de systèmes d'information. Cela étant dit, un trait de caractère du droit de la lutte contre la cybercriminalité saute aux yeux : il s'agit de sa nouveauté. En effet, les normes de l'Union dans ce domaine sont récentes. Le droit primaire reflète d'ailleurs cette évolution. Le *Traité de Maastricht*, en particulier l'art. K.1, est silencieux à l'égard de ce phénomène[4]. Il en est de même pour le *Traité d'Amsterdam* (l'art. 29 du *Traité sur l'Union européenne* (*TUE*) est davantage prolixe au sens où elle mentionne davantage de phénomènes criminels que le *Traité de Maastricht*, mais elle omet de citer la cybercriminalité)[5]. Cette dernière est mentionnée par le droit primaire dans le *Traité de Lisbonne*[6]. L'art. 83§ 1 du *Traité sur le fonctionnement de l'UE* (*TFUE*) emploie le terme de criminalité informatique[7]. Une telle formulation, désuète, puisqu'abandonnée dans le droit dérivé dès le début des années 2000 au profit de l'appellation cybercriminalité, a néanmoins le mérite de souligner l'importance accordée par l'Union à ce phénomène. Pour autant, la lutte contre ce phénomène

---

1 CE, *Communication de la Commission du 20 juin 2014 sur le rapport final sur la mise en œuvre de la stratégie de sécurité intérieure de l'UE*, [2014] JO, C 365 à la p 3.

2 CE, *Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil*, [2013] JO, L 218 à la p 8; Dans le même registre, voir la p 15 dans CE, *Communication de la commission au parlement européen, au conseil, comité économique et social européen et au comité des régions : le programme européen en matière de sécurité*, [2015] JO, C 185 [CE, *Communication sur le programme européen*].

3 CE, *Communication conjointe de la Commission et du Haut représentant du 7 février 2013 : Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé*, [2013] JO C 1 à la p 9 [CE, *Communication conjointe du 7 février 2013*].

4 Voir notamment l'art K.1 dans *Traité sur l'Union européenne,* 7 février 1992, C 326/13 (entrée en vigueur : 1er novembre 1993) [*TUE*].

5 *Traité d'Amsterdam modifiant le Traité sur l'Union européenne*, 2 octobre 1997, C 340/01, art 29 (entrée en vigueur : 1er mai 1999) [*Traité d'Amsterdam*].

6 *Traité de Lisbonne modifiant le traité sur l'Union européenne et le traité instituant la Communauté européenne*, 13 décembre 2007, C 306/23 (entrée en vigueur : 1er décembre 2009) [*Traité de Lisbonne*].

7 *Traité sur le fonctionnement de l'Union européenne*, 13 décembre 2007, C 326/01, art 83§1 (entrée en vigueur : 1er décembre 2009) [*TFUE*].

implique le recours par l'Union de différentes bases juridiques, notamment les art. 87 et 88 du *TFUE* (coopération policière)[8]. Si la cybercriminalité (ou la criminalité informatique pour être exact) est évoquée dans l'article consacré à l'harmonisation des législations pénales, il importe de garder à l'esprit que la lutte menée déborde le Chapitre 4 (coopération judiciaire en matière pénale) du titre V de la troisième partie du *TFUE*, relatif à l'espace de liberté, de sécurité et de justice (ELSJ)[9], voire au-delà, puisque la *directive sur le commerce électronique*, dont les dispositions encadrent la responsabilité de l'hébergeur quant à d'éventuels contenus illicites, repose sur des bases juridiques ayant trait au marché intérieur. Cependant, l'essentiel de cette lutte trouve son centre de gravité dans la matière pénale. À ce propos, le caractère territorial du droit pénal rend, malgré les améliorations réalisées, les outils répressifs traditionnels peu opérants[10]. Face à un phénomène d'ampleur transnational, les États membres ne peuvent agir de manière isolée. Une action européenne en matière de lutte contre la cybercriminalité émerge dès lors au fil du temps (1). Elle naît à travers l'élaboration de normes de droit dérivé, mais, pour dépasser la lecture chronologique des actes adoptés, il est possible de remarquer trois phénomènes complémentaires : il s'agit d'abord, de l'importance de l'usage des instruments de droit commun dans la lutte contre la cybercriminalité[11]. Autrement dit, les progrès effectués concernant l'espace pénal européen profitent *ipso jure* à la lutte contre la cybercriminalité. Ensuite, il existe des mesures spécifiques à cette lutte, mais bon nombre d'entre elles se trouvent dans le périmètre de la *soft law* et relève de mesures opérationnelles, c'est-à-dire menées hors du champ balisé par l'art. 288 du *TFUE*[12] relatif à la nomenclature des actes de l'Union. Enfin, la lutte contre la cybercriminalité tend, à l'heure actuelle, à se trouver à la convergence de plusieurs agendas institutionnels. Sans vouloir être exhaustif, il est possible d'en dénombrer au moins trois. Ces trois agendas favorisent une dynamique intégrative puissante (2).

I. L'émergence d'une action européenne spécifique

La prise de conscience de l'Union concernant le danger que fait peser la cybercriminalité est ancienne[13]. À l'époque, la sémantique était différente. Il était davantage question de « criminalité informatique » (A). Le terme de cybercriminalité va peu à peu s'imposer, au fur et à mesure que l'action de l'Union se singularise (B).

---

8 *Ibid*, arts 87 et 88.

9 *TUE*, *supra* note 4, Chap 4, titre 5.

10 Myriam Quéméner et Joël Ferry, *Cybercriminalité : Défi mondial*, 2e éd, Paris, Economica, 2009 à la p 244.

11 C'est un aspect qui ne sera pas évoqué dans cette étude, mais qui est clairement rappelé par le Parlement européen dans sa résolution, à savoir que la lutte contre la cybercriminalité se doit de respecter les garanties procédurales de droit commun. CE, *Résolution du Parlement européen du 3 octobre 2017 sur la lutte contre la cybercriminalité*, [2017] JO, C 366 considérant qu'à ce titre, les avancées dans le droit lié à l'harmonisation européenne sont applicables à ce domaine.

12 *Traité de Lisbonne*, *supra* note 6, art 288.

13 Quéméner et Ferry, *supra* note 10 à la p 260.

A. De la lutte contre la « criminalité informatique » à la lutte contre la cybercriminalité

La criminalité est un thème mis à l'agenda des institutions de l'Union au tournant des années 2000. Le *Traité d'Amsterdam* n'évoque pas explicitement la lutte contre ce phénomène. L'article 29 *TUE* mentionne seulement des phénomènes adjacents, notamment la criminalité organisée et les crimes commis contre des enfants[14]. Il en est de même pour le programme d'action relatif à la criminalité organisée adopté par le Conseil le 28 avril 1997[15].

Ce thème de la criminalité informatique va être abordé à partir des années 2000. Le terrain est propice à une action institutionnelle. La Commission avait commandé une étude dénommée COMCRIME présentée par elle par la suite, au Conseil en avril 1998. Cette étude, réalisée par l'Université de Würzburg en Allemagne, a mis en avant la vulnérabilité de la société de l'information à l'égard de la criminalité informatique[16]. Considérant qu'il s'agit d'une menace majeure à celle-ci, elle préconisait une action de nature globale et internationale. Sa publication est intervenue au moment où les premiers travaux à l'échelon international se sont déroulés contre ce phénomène. Le G8 a instauré un Groupe d'experts à haut niveau sur la criminalité transnationale (dénommé « Groupe de Lyon ») sur la base des recommandations approuvées à Lyon par les chefs d'État en 1996. Figurait dans le mandat de ce groupe d'experts, l'établissement de normes, de principes, de bonnes pratiques en matière de criminalité informatique, comme forme particulière de la criminalité organisée transnationale. En outre, les ministres de la Justice et des Affaires intérieures du G8, lors de leur rencontre les 9 et 10 décembre 1997, à Washington DC, aux États-Unis, ont approuvé les principes fondateurs du réseau de points de contact nationaux spécialisés dans la lutte contre la criminalité liée à la haute technologie[17]. Par ailleurs, une conférence du G8 s'est tenue à Paris du 15 au 17 mai 2000, intitulée « Instaurer la confiance et la sécurité dans le cyberespace ».

La période correspondant à la fin des années 1990 et au début des années 2000 est donc celle d'une intense activité institutionnelle, non seulement au sein du G8 et de son groupe de travail, mais aussi dans d'autres sphères, en l'occurrence le Conseil de l'Europe et l'Union européenne.

Le Conseil de l'UE a adopté en 1999 une position commune[18], quant à une

---

14 *TUE*, *supra* note 4, art 29.

15 CE, *Programme d'action relatif à la criminalité organisée*, [1997] JO, C 251/01 à la p 1. Il en est d'ailleurs de même dans CE, *Résolution du Conseil du 21 décembre 1998 relative à la prévention de la criminalité organisée en vue de l'établissement d'une stratégie globale de lutte contre cette criminalité*, [1998] JO, C 408.

16 Ulrich Sieber, « Legal Aspects of Computer-related Crime in the Information Society — COMCRIME » (1998) Université de Würzburg, Document de travail 1.0, en ligne : OAS <www.oas.org/juridico/english/COMCRIME%20Study.pdf>.

17 Qui a débouché sur l'adoption par le Conseil de CE, *Recommandation du conseil du 25 juin 2001 concernant les points de contact assurant un service vingt-quatre heures sur vingt-quatre pour lutter contre la criminalité liée à la haute technologie*, [2001] JO, C 187/02 à la p 5.

18 CE, *Position commune 1999/664/JAI du 27 mai 1999, arrêtée par le Conseil sur la base de l'article 34 du traité sur l'Union européenne, concernant les négociations relatives au projet de convention sur la*

convention, dénommée convention du Budapest, visant à mener, en priorité, une politique pénale commune destinée à protéger la société de la criminalité dans le cyberespace, notamment par l'adoption d'une législation appropriée et par l'amélioration de la coopération internationale[19]. Ce texte, ouvert à la signature le 23 novembre 2001, sera le premier texte juridique contraignant d'envergure paneuropéenne destiné à lutter contre la criminalité informatique[20].

Un rapport de l'Assemblée parlementaire du Conseil de l'Europe décrit parfaitement la situation au tournant des années 2000. Quasiment inexistant dans les années 80 et au début des années 90, le recours aux nouvelles technologies de l'information est à présent monnaie courante. La collaboration multilatérale internationale se révèle dès lors impérieuse dans la mesure où si Internet ne connaît pas de frontières, la criminalité informatique n'en connaît pas non plus[21].

La nécessité de réprimer efficacement la criminalité informatique a conduit les chefs d'État et de gouvernement à émettre le souhait, au cours du Conseil européen de Tampere de 1999, que l'Union se concentre sur la criminalité utilisant les technologies avancées, en trouvant un accord sur des définitions, des incriminations et des sanctions communes face à ce phénomène[22]. Ces mêmes chefs d'État et de gouvernement ont demandé, en mars 2000, l'établissement d'un plan d'action dénommé *Europe* destiné à dynamiser l'économie européenne. Ce plan global d'action préparé par la Commission et le Conseil, et approuvé par le Conseil européen à Feira en juin 2000, comprend un volet relatif à la criminalité informatique. La lutte contre ce phénomène apparaît donc comme un complément aux efforts menés dans le cadre du marché intérieur.

Quant aux ministres de l'Intérieur et de la Justice, ils ont souligné, lors du Conseil Justice et Affaires intérieures (JAI) informel de Marseille des 28 et 29 juillet 2000, l'importance d'une initiative de l'Union européenne en la matière. Il s'agit en l'occurrence d'étendre le mandat d'Europol à la criminalité informatique[23]. Dans le

---

criminalité dans le cyberespace, qui sont menées au sein du Conseil de l'Europe, [1999] JO, L 142 à la p 1.

19 Le troisième considérant la *Convention de Budapest sur la cybercriminalité*, 23 novembre 2011, STE n° 185 (entrée en vigueur : 1er juillet 2004).

20 Dont une présentation est faite dans : Kristian Bartholin, « La Convention de Budapest sur la cybercriminalité du 23 novembre 2001 » dans Irène Bouhadana et William Gilles, dirs, *Cybercriminalité, cybermenaces et cyberfraudes*, Paris, Institut du Monde et du Développement, 2012 aux pp 95-99.

21 CE, AP, 2001 sess ordinaire, *Lutte de l'Europe contre la criminalité économique et le crime organisé transnational : progrès ou recul?*, Rapport, vol 5, Doc 9018 (2001) à la p 107.

22 Voir le point 48 dans CE, Parlement européen, *Conclusions de la présidence du Conseil européen de Tampere des 15 et 16 octobre 1999*, Finlande, CE, 1999.

23 CE, Justice et Affaires intérieures (JAI), *Proposition d'extension du mandat d'Europol à la lutte contre la cybercriminalité : note de la Présidence au Comité de l'article 36*, Conseil du 12 octobre 2000, Doc 12224/00 EUROPOL 31 (2000); Ce qui sera fait peu après puisque depuis l'entrée en vigueur de CE, *Décision du Conseil du 6 décembre 2001 étendant le mandat d'Europol à la lutte contre les formes graves de criminalité internationale énumérées à l'annexe de la convention Europol,* [2001] JO, C 362/01; Europol est compétent pour toutes les formes de criminalité énumérées à l'annexe de la *Convention de 1995* : CE, *Convention Europol*, 26 juillet 1995, C 316/48 (entrée en vigueur : 26 juillet 1995), figure dans cette liste de 25 types d'infractions, la criminalité informatique.

programme de la présidence française pour les relations extérieures dans le domaine de la justice et des affaires intérieures, celle-ci indique qu'elle

> mettra également l'accent sur le renforcement des instruments de lutte contre la criminalité organisée, le blanchiment et la cybercriminalité, s'agissant là d'un enjeu majeur pour la réalisation de l'espace de liberté, de sécurité et de justice[24].

Au cours de cette année, la cybercriminalité se trouve à la jonction de deux projets de l'Union, l'ELSJ d'une part, la société numérique d'autre part. Une communication du 26 janvier 2001 s'interroge sur la manière de lutter contre ce phénomène dans le contexte de la promotion d'une économie numérique et de la création l'ELSJ[25]. Il souligne les lacunes en matière de lutte contre la criminalité informatique, en particulier l'absence de statistiques fiables sur l'étendue du phénomène. Surtout, il est intitulé « Créer une société de l'information plus sûre en renforçant la sécurité des infrastructures de l'information et en luttant contre la cybercriminalité ». Le terme de cybercriminalité est désormais privilégié. Il va connaître une fortune incontestable.

B. L'ébauche d'une action européenne singulière

Si les années 1990 correspondent au temps des premières mesures, les années suivantes vont révéler une intensification de la lutte contre ce qu'il convient à présent d'appeler donc la cybercriminalité. Sur le plan pénal, la Commission européenne propose un rapprochement des normes de droit national relatives aux infractions ayant trait à ce phénomène, de même qu'un niveau de protection minimum des victimes de ce type de criminalité, notamment les victimes de la cyberpornographie[26]. Diverses questions se posent telles que l'adaptation du droit européen existant, en particulier la *Convention de 2000 relative à l'entraide*

---

[24] Voir le point 2 dans CE, Justice et Affaires intérieures (JAI), *Programme de la Présidence française pour les relations extérieures dans le domaine JAI*, Conseil du 6 juillet 2000, Doc 10135/00 JAI 75.

[25] CE, Commission, *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 - eEurope 2002*, [2000] COM 890.

[26] La lutte contre la cyberpornographie est un thème précurseur de la lutte contre la cybercriminalité. Avec la criminalité organisée transnationale, il est possible de considérer qu'il s'agit du sujet ayant amené la Communauté (et l'Union) européenne(s) à s'intéresser à la commission de délits commis au moyen d'ordinateurs. Voir à ce sujet CE, *Déclaration du Conseil et des ministres de l'éducation réunis au sein du Conseil du 20 décembre 1996 sur la protection des enfants et la lutte contre la pédophilie*, [1997] JO, C7 à la p 12; CE, *Recommandation du Conseil le 24 septembre 1998, concernant le développement de la compétitivité de l'industrie européenne des services audiovisuels et d'information par la promotion de cadres nationaux visant à assurer un niveau comparable et efficace de protection des mineurs et de la dignité humaine*, [1998] JO, L 270 à la p 48; CE, *Décision n° 276/1999/CE du Parlement européen et du Conseil du 25 janvier 1999 adoptant un plan d'action communautaire pluriannuel visant à promouvoir une utilisation plus sûre d'Internet par la lutte contre les messages à contenu illicite et préjudiciable diffusés sur les réseaux mondiaux*, [1999] JO, L 33 à la p 1; CE, *Décision du Conseil du 29 mai 2000 relative à la lutte contre la pédopornographie sur l'Internet*, [2000] JO, L 138 à la p 1.

judiciaire[27]. Même si ce texte est neutre sur le plan technologique, la Commission émet l'idée qu'il importe de voir à l'expérience son utilité. De surcroît, elle s'interroge sur l'idée de dépasser les standards posés par la *Convention de Budapest*. Cette communication marque une étape importante, car elle identifie la cybercriminalité comme une problématique à part entière requérant un ensemble de mesures pour contrer un tel phénomène. Les années qui vont suivre vont donner lieu à l'adoption de différents textes destinés à mieux réprimer la cybercriminalité. Elles vont en effet voir se concrétiser l'adoption de plusieurs normes de droit spécial, en particulier concernant la pédopornographie en 2003 (un projet de décision-cadre ayant été présenté par la Commission quelques semaines avant sa communication de 2001)[28] et une autre concernant les attaques visant les systèmes d'information en 2005 (un projet de décision-cadre ayant été présenté par la Commission le 19 avril 2002). À l'appui du rapprochement des législations opéré, ce texte de 2005 constate que

> les systèmes d'information font l'objet d'attaques, notamment dues à la criminalité organisée, et que l'inquiétude croît face à l'éventualité d'attaques terroristes contre les systèmes d'information qui font partie de l'infrastructure critique des États membres. Cette situation risque de compromettre la réalisation d'une société de l'information plus sûre et d'un espace de liberté, de sécurité et de justice, et appelle donc une réaction au niveau de l'Union européenne[29].

Un tel document est de portée majeure dans la mesure où il constitue, du point de vue du droit de l'Union, le premier texte destiné à harmoniser les droits nationaux afin de lutter contre la cybercriminalité. Il prévoit des incriminations et des sanctions communes ayant trait à l'intrusion dans un système d'information, à l'atteinte à l'intégrité d'un système ainsi qu'aux atteintes à l'intégrité des données. Il s'agit ainsi de réprimer des pratiques telles que le *phreaking*, le *mailbombin*g ou la contamination par des vers ou des virus informatiques[30].

En parallèle, les progrès réalisés dans l'édification de l'espace pénal européen ont des répercussions concrètes en matière de lutte contre la cybercriminalité. En effet, des instruments, tels que le mandat d'arrêt européen ou la reconnaissance mutuelle des décisions de gel des avoirs criminels, englobent la cybercriminalité dans leur champ d'application[31]. Il en est par ailleurs de même

---

27 *Convention du 29 mai 2000 relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne*, 29 mai 2000, JO C 197/1 à la p 1 (entrée en vigueur : 23 août 2005).

28 CE, *Décision-cadre 2004/68/JAI du Conseil du 22 décembre 2003 relative à la lutte contre l'exploitation sexuelle des enfants et la pédopornographie*, [2004] JO, L 13 aux pp 44-48.

29 CE, *Décision-cadre 2005/222/JAI du Conseil du 24 février 2005 relative aux attaques visant les systèmes d'information*, [2007] JO, L 69 à la p 67.

30 Le *phreaking* est une technique informatique consistant à faire usage d'un système de manière non prévue par son opérateur, le but tant d'obtenir gratuitement des services ou d'avoir accès à des fonctions non autorisées. Le *mail-bombing* est une technique d'attaque consistant à envoyer massivement des courriels à une boîte de mail de sorte de rendre celle-ci inopérante.

31 CE, *Décision-cadre 2002/584/JAI du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres*, [2002] JO, L 190 à la p 1; CE, *Décision-cadre 2003/577/JAI du Conseil du 22 juillet 2003 relative à l'exécution dans l'Union européenne des décisions de gel de biens ou d'éléments de preuve*, [2003] JO, L 196 à la p 45; CE, *Décision-cadre*

concernant *Eurojust* qui voit son mandat élargi à ce type de phénomène[32]. Dans un registre similaire, les premières avancées en matière d'harmonisation du droit des victimes de la criminalité profitent indirectement à celles de la cybercriminalité[33].

Le nouveau programme quinquennal concernant le développement de l'ELSJ, le programme de La Haye, n'aborde pas la question de la cybercriminalité. Cependant, ce texte approuvé par les chefs d'État et de gouvernement les 4 et 5 novembre 2004 s'inscrit en toile de fond de préoccupations sécuritaires fortes. Comme l'indiquent les conclusions établissant ce programme, la question de la sécurité de l'Union et de ses États membres se pose avec une acuité au regard des attentats terroristes de Madrid perpétrés le 11 mars 2004. Quant aux attaques de Londres, elles vont exacerber cette situation et c'est d'ailleurs peu après que la directive dite « rétention », destinée à définir une durée de conservation harmonisée à l'attention des fournisseurs de réseaux et de services, va faire l'objet d'une approbation politique au sein du Conseil et d'un accord entre ce dernier et le Parlement européen, l'objectif étant de mettre à disposition les données relatives aux communications électroniques aux autorités pénales nationales[34]. La lutte contre la cybercriminalité va demeurer au-devant de la scène peu de temps après, en 2007 avec la présentation d'une nouvelle communication.

II. Une action substantielle sujette à une dynamique intégrative puissante

À l'instar des autres politiques de l'Union, l'action menée dans le domaine de la lutte contre la cybercriminalité peut s'analyser sous le prisme néofonctionnaliste : la gravité du danger fait naître un besoin pour l'Union et les États membres d'intervenir dans un domaine donné. Cette intervention menée au nom des nécessités du moment se réalise par le recours aux bases juridiques existantes du traité, en élaborant des normes de droit dérivé. Une telle action tend à se densifier au fil de l'élaboration de ces normes (A). L'une des raisons de ce phénomène tient au fait que la lutte contre la cybercriminalité se trouve à la jonction de trois agendas institutionnels distincts (B). En se situant au point de convergence, elle tire profit des mouvements d'intégration créés par ces trois agendas.

2005/214/JAI du Conseil du 24 février 2005 concernant l'application du principe de reconnaissance mutuelle aux sanctions pécuniaires, [2005] JO, L 76 à la p 16.

32 Voir l'art 4§1 alinéa b dans CE, *Décision 2002/187/JAI du Conseil du 28 février 2002 instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité*, [2002] JO, L 63 à la p 1.

33 CE, *Décision-cadre 2001/220/JAI du Conseil du 15 mars 2001 relative au statut des victimes dans le cadre de procédures* pénales, [2001] JO, L 82 à la p 1.

34 CE, *Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE*, [2006] JO, L 105 à la p 54.

A. Un processus de densification normative

La lutte contre la cybercriminalité souffre d'une fragmentation normative inhérente à l'existence de fondements juridiques éparpillés dans diverses politiques de l'Union. Certes, ce constat vaut pour les différents domaines d'action de l'Union, ceci au vu de la diversité des bases juridiques et des procédures législatives applicables. Cependant, le clivage entre piliers aggrave le phénomène, multipliant le risque de conflit institutionnel et brouillant la lisibilité de l'action juridique menée au vu de la prolifération d'instruments soumis à des régimes juridiques spécifiques[35]. Le risque est donc un morcellement politique de l'action européenne. Consciente de ce danger, l'Union s'efforce de l'organiser de manière rationnelle, à partir d'un ensemble de mesures ambitieuses.

Une nouvelle communication présentée en 2007 souligne l'importance d'aller plus loin dans la lutte contre la cybercriminalité. Elle part du constat selon lequel le nombre de délits informatiques est en augmentation, les activités criminelles s'internationalisent et se sophistiquent, les groupes criminels organisés sont impliqués de plus en plus dans ce type de délits et enfin le nombre des poursuites engagées dans l'Union dans le cadre de la coopération transfrontalière stagne[36]. C'est pourquoi elle préconise un ensemble de mesures pour renforcer la lutte contre ce phénomène[37].

En réponse à cette communication visant « désormais approfondir la politique générale de lutte contre la cybercriminalité[38] », le Conseil a adopté des conclusions le 27 novembre 2008 dans lesquelles il envisage l'adoption de mesures à court terme destinées à lutter contre la cybercriminalité, comme la création d'une plateforme européenne de signalement des faits ou bien encore le recours aux équipes communes d'enquêtes. Ces conclusions, qui constatent que les infractions commises sur Internet sont en augmentation constante et sont de plus en plus transnationales, évoquent également des mesures à plus long terme, telles que la facilitation des perquisitions à distance et le développement d'indicateurs statistiques[39].

Les mesures prévues par les conclusions du Conseil, établissant une stratégie de travail concertée et des mesures concrètes de lutte contre la cybercriminalité, sont

---

35 Pour une critique de cette fragmentation, voir Ramses A. Wessels, « Towards EU Cybersecurity Law: Regulating a New Policy Field » dans Nikolaos K. Tsagourias, Russell Buchan, dirs, *International Law and Cyberspace*, Cheltenham, Edward Elgar Publishing, 2015 aux pp 414-415.

36 CE, *Communication du 22 juin 2007 intitulée : vers une politique générale en matière de lutte contre la cybercriminalité*, [2007] JO, COM 267 à la p 3 [CE, *Communication du 22 juin 2007*].

37 Telles qu'aider financièrement la formation des services répressifs chargés de la lutte contre la cybercriminalité, promouvoir la recherche dans ce domaine, élaborer une réglementation relative à l'usurpation d'identité, améliorer les méthodes de lutte contre la fraude et le commerce illicite sur Internet, faciliter le dialogue avec l'industrie dans le cadre d'un forum européen pour la sécurité, la recherche et l'innovation, et permettre l'élaboration de statistiques communes ou encore la promotion d'accords entre les pouvoirs publics et les opérateurs privés, destinés à bloquer des sites Internet illégaux.

38 CE, *Communication du 22 juin 2007*, *supra* note 36 à la p 9.

39 CE, *Conclusions du Conseil du 27 novembre 2008 relatives à une stratégie de travail concertée et à des mesures concrètes de lutte contre la cybercriminalité*, [2008] JO, C 62 à la p 16 [CE, *Conclusions du Conseil du 27 novembre 2008*].

relayées et complétées par le programme de Stockholm approuvé par le Conseil européen le 11 décembre 2009[40]. Ces conclusions fixent un ensemble de priorités sur la cybercriminalité, notamment, la production par Europol d'une analyse stratégique concernant ce phénomène et la présentation par la Commission de propositions relatives au cadre juridique en matière d'enquêtes dans le cyberespace[41].

Les mesures prévues par ce programme de Stockholm qui prend la suite du programme de La Haye sont reprises et développées dans le plan d'action ayant pour objectif de mettre en œuvre la stratégie concertée de lutte contre la cybercriminalité[42]. Le plan d'action qui complète la stratégie concertée fait remarquer le fait qu'en raison du caractère transnational de la cybercriminalité, il importe de renforcer sensiblement la coopération entre les États membres. C'est pourquoi, il contient un ensemble de mesures, notamment la mise en place ou l'adaptation de dispositifs nationaux en vue de permettre les notifications à la plateforme de lutte contre la cybercriminalité gérée par Europol, la ratification par tous les États membres de la convention de Budapest, une harmonisation des différents réseaux fonctionnant 24 heures sur 24, et la mise en place par les États membres de cyberpatrouilles. L'action de l'Union dans ce domaine se densifie, au gré des actes législatifs et des mesures opérationnelles. Il reste que la lutte contre la cybercriminalité se voit stimulée par divers agendas institutionnels qui tendent à interagir.

La dynamique institutionnelle se traduit par cette densification normative progressive, manifestation du processus d'engrenage à l'œuvre. Sans vouloir être exhaustif, la théorie néofonctionnaliste, bien connue des juristes de droit européen, se caractérise par des phénomènes de débordement, c'est-à-dire l'intrusion de l'intégration européenne dans de nouveaux domaines. La complexité de la construction européenne tient au fait que le phénomène global d'intégration se décompose en processus sectoriels, qui tendent à superposer. L'image de mouvements d'ondes provenant de directions différentes permet de mieux appréhender un tel phénomène. Ces ondes se rencontrent et, par effet de résonance, elles se conjuguent pour prendre de l'amplitude. La lutte contre la cybercriminalité se trouve à la jonction de trois agendas institutionnels distincts. Ce point de convergence lui permet de bénéficier des mouvements d'intégration générés par ces trois agendas qui, loin d'être séparés, interagissent fortement. Cette intrication se traduit par l'élaboration un processus de renforcement réciproque des normes juridiques, les textes adoptés dans un domaine servant de marchepied à l'élaboration de projets menés dans d'autres.

---

40 CE, *Programme de Stockholm : une Europe ouverte et sûre qui sert et protège les citoyens*, [2010] JO, C 115 à la p 1 [CE, *Programme de Stockholm*].

41 CE, *Conclusions du Conseil du 27 novembre 2008*, *supra* note 39, point 4.4.4.

42 Conseil de l'Europe, *Projet de conclusions du Conseil relatives à un plan d'action visant à mettre en œuvre la stratégie concertée de lutte contre la cybercriminalité*, Conseil du 25 mars 2010, Doc 5957/2/10, CRIMORG 22, ENFOPOL 32.

B. Une action à la convergence de plusieurs agendas institutionnels

Mis à part l'espace pénal européen qui mériterait à lui seul de nombreux développements[43], la lutte contre la cybercriminalité se trouve à la confluence de trois agendas européens distincts : le marché numérique européen, la cybersécurité et la sécurité intérieure.

Le premier d'entre eux a trait en effet au marché numérique européen comme levier de croissance de l'économie européenne. En 2010 a été lancée la stratégie numérique destinée à stimuler cette économie par le biais de la promotion de ce type de marché. Deux années plus tard, en 2012 donc, la Commission a présenté une communication constatant que lors des vingt dernières années, l'économie numérique constitue un moteur non négligeable de la croissance et, surtout qu'elle devrait croître de manière exponentielle les années suivantes[44]. Elle a présenté, en avril 2015, une *Stratégie pour un marché unique numérique en Europe***.** Dans ce texte, elle considère que « la technologie de l'information et des communications (TIC) ne sont plus un secteur économique parmi d'autres, mais elles constituent désormais la base sur laquelle reposent tous les systèmes économiques novateurs modernes[45] ». C'est la raison pour laquelle elle suggère de créer un marché unique numérique connecté qui est la transposition du marché unique au cyberespace. Comme l'indique la Commission, cet espace correspond à celui au sein duquel les particuliers et les entreprises peuvent accéder et se livrer à des activités en ligne de manière sûre, c'est-à-dire par des règles européennes garantissant à la fois une concurrence loyale et une protection des consommateurs. La cybercriminalité n'est pas éludée puisqu'elle relève des failles spécifiques dans ce secteur en mutation rapide. Le contrôleur européen de la protection des données (CEPD) qualifie à ce sujet la lutte contre la cybercriminalité comme « une pierre angulaire du renforcement de la sécurité et de la sûreté dans l'espace numérique et de l'instauration de la confiance nécessaire[46] ». La cybercriminalité est donc un phénomène mettant en danger le développement du marché intérieur, tout comme la criminalité organisée était, dans les années 1980, un phénomène menaçant l'essor du marché unique justifiant, dans les années 1990, l'octroi à l'Union des compétences en matière répressive.

Quant au Parlement européen, il approuve en 2016 l'idée de ce marché unique numérique de manière à rendre l'Union compétitive dans le domaine de l'économie numérique. Il salue la création de l'unité anticybercriminalité d'Europol (EC3), il préconise l'usage du cryptage par les citoyens et les entreprises pour protéger leur vie privée et sécuriser leurs communications, et il rappelle que la

---

43 Ce thème a été traité par nos soins dans le cadre d'une étude spécifique : « Aperçus de la lutte contre la cybercriminalité dans l'Union européenne » (2018) 2 Revue de sciences criminelles et de droit pénal comparé 59.

44 CE*, Communication de la Commission du 18 décembre 2012 sur le contenu dans le marché unique numérique*, [2012] JO, COM 789.

45 CE, *Communication de la Commission du 6 mai 2015 : Stratégie pour un marché unique numérique en Europe*, [2015] JO, COM 192.

46 Voir art 3§50 dans CE, *Résumé de l'avis du Contrôleur européen de la protection des données relatif à la communication de la Commission européenne au Conseil et au Parlement européen concernant l'établissement d'un Centre européen de lutte contre la cybercriminalité*, [2012] JO, C 336 à la p 7.

sécurité dans le cyberespace constitue un impératif dans l'établissement de cette confiance, faute de quoi, il n'y aurait pas de marché unique numérique compétitif[47]. Surtout, le Parlement souligne deux aspects importants, à savoir une meilleure résistance face aux cyberattaques grâce au renforcement de l'Agence européenne de sécurité des réseaux (ENISA), ainsi qu'une réponse harmonisée de la part de l'Union et de ses États membres grâce à une stratégie commune et l'application rapide de la *directive « SRI »*.

Ces recommandations font écho à un deuxième agenda institutionnel dans lequel s'inscrit la lutte contre la cybercriminalité, à savoir la cybersécurité. Le Haut-représentant et la Commission européenne ont présenté, le 7 février 2013, une stratégie de cybersécurité qui énonce que le monde numérique, s'il procure d'énormes avantages, est aussi très vulnérable. Les incidents de cybersécurité, d'origine malveillante ou accidentelle, se multiplient à un rythme inquiétant et pourraient perturber la fourniture de services essentiels que nous tenons pour acquis comme l'eau, les soins de santé, l'électricité ou les services mobiles[48].

Cette stratégie évoque la cybercriminalité dont la sophistication des méthodes constitue une menace pour un cyberespace ouvert et sûr. Une telle stratégie vise à étendre les valeurs de l'Union présentes dans le « monde physique », au sein du « monde numérique[49] ». Elle s'accompagne pour ce faire d'une proposition de directive adoptée au demeurant, le 6 juillet 2016[50]. Cette directive dite « SRI » ou « NIS » part du principe que la sécurité des réseaux est un maillon indispensable au fonctionnement du marché intérieur (ce qui explique au demeurant la mention du thème de la sécurité des réseaux par la *Stratégie de 2015 pour un marché unique numérique en Europe*). Elle précise que de par son caractère transnational, toute perturbation importante de ces réseaux a une incidence sur plusieurs États membres ainsi que sur l'Union dans son ensemble. Or, les incidents se multiplient, ceux-ci étant parfois le fruit d'actions intentionnelles malveillantes, portant préjudice à la confiance numérique[51]. Aussi, cette directive entend harmoniser et élever le niveau de sécurité des réseaux[52]. Elle prévoit toute une série d'obligations à l'égard des États membres : établissement d'une stratégie nationale établissant des objectifs et des mesures en matière de cybersécurité, renforcement des capacités de réponse aux incidents de sécurité informatique (CSIRT) nationaux et obligation de notification d'incidents à l'égard des opérateurs de services essentiels (OSE). En réalité, cette directive doit se comprendre comme un premier pas, tout comme la cyberstratégie de 2013 dont les axes méritent d'être davantage précisés et structurés. C'est d'ailleurs la raison pour

---

47 Voir arts 3.4§87-93 dans CE, *Résolution du Parlement européen du 19 janvier 2016 : Vers un acte sur le marché unique numérique*, [2016] JO, C 11/55.

48 CE, *Communication conjointe du 7 février 2013*, *supra* note 3 à la p 3.

49 *Wessels*, *supra* note 35 à la p 411.

50 CE, *Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union*, [2016] JO, L 194 à la p 1.

51 *Ibid*, arts 2 et 3.

52 Myriam Quéméner, « La directive NIS, un texte majeur en matière de cybersécurité » (2016) 23:3 Sécurité et stratégie 50 à la p 51.

laquelle cette stratégie a été actualisée en 2017[53]. La nouvelle note que la sécurité future dépend de la manière dont l'Union saura se protéger des cybermenaces. Constatant l'aggravation de la cybercriminalité et conjecturant l'accentuation de ce phénomène, une telle stratégie promeut de nouvelles mesures à l'encontre de leurs auteurs. Dans le volet « cyberdissuasion » de la stratégie, cette dernière recense un ensemble de mesures, parmi lesquelles un renforcement des prérogatives d'Europol en matière de cybercriminalistique et de surveillance du *darknet*, et un financement de projets visant améliorer la justice pénale dans le cyberespace. Le Conseil a approuvé, le 20 novembre 2017, cette stratégie en soulignant que le « niveau élevé de cyberrésilience dans toute l'UE est également important pour assurer la confiance dans le marché unique numérique et la poursuite du développement d'une Europe numérique[54] ». Les conclusions du Conseil attestent du fait que marché unique numérique et cybersécurité sont des domaines sécants.

En réalité, ce sont les agendas relatifs respectivement à l'économie numérique, à la cybersécurité et à la sécurité intérieure, qui tendent à se chevaucher. La cybercriminalité se trouve en effet au point de jonction entre divers agendas qui s'entrecroisent : l'économie numérique et la cybersécurité certes, mais aussi la sécurité intérieure. Dans son programme européen en matière de sécurité (qui est le document préparatoire la stratégie européenne de sécurité intérieure pour la période 2010-2015), la Commission avait déclaré à ce sujet que la cybersécurité constitue la première ligne de défense contre la cybercriminalité[55]. La stratégie européenne approuvée par le Conseil de l'UE les 25 et 26 février 2010, puis par le Conseil européen les 25 et 26 mars 2010 constate que la « cybercriminalité représente une menace mondiale, technique, transfrontière et anonyme pour nos systèmes d'information et de ce fait, elle pose de nombreux défis supplémentaires aux autorités policières[56] ». Cette stratégie, qui répond au souhait des chefs d'État et de gouvernement dans le *programme de Stockholm de 2009*[57], place la lutte contre la cybercriminalité comme un objectif prioritaire. Elle détermine les grands principes d'une action européenne dans ce domaine. Ce texte a été complété par une communication de la Commission publiée le 22 novembre 2010 qui énonce les cinq objectifs de l'action européenne pour la période 2010-2015[58]. Or, figure parmi ces objectifs, la lutte contre la cybercriminalité. Plus exactement, l'objectif n° 3 est intitulé « accroître le niveau de sécurité des citoyens et des entreprises dans le cyberespace » et à l'appui de cet objectif, la Commission note que la cybercriminalité constitue un phénomène mondial préjudiciable pour le marché intérieur européen.

---

53 CE, *Communication du 13 septembre 2017 : Résilience, dissuasion et défense : doter l'UE d'une cybersécurité solide*, [2017] JO, C 450.

54 CE, *Conclusions du Conseil sur la communication conjointe au Parlement européen et au Conseil - Résilience, dissuasion et défense : doter l'Union européenne d'une cybersécurité solide*, Doc 14435/17, Bruxelles, 2017 à la p 2.

55 CE, *Communication sur le programme européenne*, *supra* note 2 à la p 22.

56 Conseil de l'UE, *Projet de stratégie de sécurité intérieure pour l'Union européenne : " Vers un modèle européen de sécurité "*, Conseil du 23 février 2010, Doc 5842/1/10 JAI 90 à la p 6.

57 CE, *Programme de Stockholm*, *supra* note 40.

58 CE, *Communication de la Commission du 22 novembre 2010 : La stratégie de sécurité intérieure de l'UE en action cinq étapes vers une Europe plus sûre*, [2010] COM 673.

La lutte contre la cybercriminalité bénéficie de l'impulsion politique très forte en matière de sécurité intérieure. Le souhait de progresser dans ce domaine se traduit par un acquis normatif conséquent, répertorié par la Commission, que ce soit dans le cadre de la stratégie 2010-2015, que dans celui de la stratégie 2010-2015. Celle-ci dresse en effet un bilan mensuel des progrès réalisés, en faisant état des actes présentés, adoptés ou en discussion. Ces rapports mentionnent régulièrement le thème de la cybercriminalité. Il faut dire que la stratégie renouvelée pour la période 2015-2020 approuvée par le Conseil dans des conclusions du 6 juin 2015 puis par le Conseil européen les 25 et 26 juin 2015 maintient la cybercriminalité comme un objectif prioritaire. Elle recense en effet parmi les priorités dans le domaine de la sécurité intérieure de l'Union européenne, la lutte contre la cybercriminalité et le renforcement de la cybersécurité[59]. Cette stratégie fait écho aux préconisations de la Commission formulées dans son programme européen en matière de sécurité, le 28 avril 2015, à savoir ériger la cybercriminalité en priorité[60]. Le Conseil a rappelé l'importance de la lutte contre la cybercriminalité. Dans des conclusions approuvées le 12 et 13 octobre 2017 sur l'examen à mi-parcours de la stratégie de sécurité intérieure renouvelée pour l'UE 2015-2020, il identifie trois priorités majeures autour desquelles l'Union doit concentrer ses efforts, à savoir le terrorisme, la prévention de la grande criminalité organisée et la cybercriminalité. Concernant cette dernière, il suggère notamment de renforcer la lutte contre ce phénomène en analysant régulièrement le tableau des différentes menaces et en veillant à la disponibilité d'outils d'investigation performants, notamment en assurant l'accès transfrontière aux preuves électroniques[61]. Cette question fait partie des problématiques actuellement traitées dans le cadre de la répression de la cybercriminalité.

***

En conclusion, il convient de retenir le fait que la lutte contre la cybercriminalité s'inscrit désormais dans une vaste gamme d'agendas institutionnels allant de la sécurité intérieure à l'espace pénal en passant par le marché numérique européen. À cet égard, la densification du tissu économique et industriel européen est actuellement une priorité pour l'Union. Un programme européen dénommé « Digital Europe[62] » vise à favoriser la recherche et l'innovation (R&I) en vue de stimuler la productivité et la compétitivité des entreprises. Constatant que « la cybercriminalité est en augmentation et les risques qu'elle comporte se diversifient à mesure que

---

59 CE, *Communication de la commission au parlement européen, au conseil, comité économique et social européen et au comité des régions : le programme européen en matière de sécurité*, [2015] JO, 185 à la p 6.

60 *Ibid* aux pp 22-24.

61 CE, *Conclusions du Conseil sur l'examen à mi-parcours de la stratégie de sécurité intérieure renouvelée pour l'Union européenne 2015-2020*, Doc 13319/17, Bruxelles, 2017 à la p 6.

62 Commission européenne, Proposition de décision du 7 juin 2018 établissant le programme spécifique d'exécution du programme-cadre pour la recherche et l'innovation «Horizon Europe» (COM(2018) 436).

l'économie et la société se numérisent », il entend protéger les citoyens contre les menaces sur la sécurité provenant d'activités criminelles. Il ajoute également la protection contre les cyberattaques ainsi que les menaces hybrides. Ces préoccupations sont croissantes à l'heure actuelle, si bien qu'un nouvel agenda de l'Union émerge, favorisant de nouvelles actions de l'Union en matière de la lutte contre la cybercriminalité. Il s'agit de la cyberdéfense. La stratégie de 2017 sur la cybersécurité, qui instaure deux piliers, d'une part, la cyberdissuasion (orientée autour de la lutte contre la cybercriminalité) et d'autre part, la cyberrésilience (axée autour de la gestion des cyberattaques), s'inscrit dans la perspective de la création d'une cyberdéfense européenne. L'idée qui sous-tend cette approche est que le cyberespace doit être protégé contre divers types de menaces considérées de manière englobante comme des actes de cybermalveillance. Une telle approche, fondée sur les thèses de la sécurité globale, est reflétée parfaitement dans le programme européen « Digital Europe » pour qui il est nécessaire de protéger les citoyens contre toutes sortes de menaces, parmi lesquelles les activités criminelles, notamment cybercriminelles, de même que les menaces hybrides, et de répondre à ces menaces en préservant les personnes, les espaces publics et les infrastructures critiques contre les cyberattaques. Le programme note en effet que les « actes de cybermalveillance menacent non seulement nos économies, mais aussi le fonctionnement même de nos démocraties, nos libertés et nos valeurs. Les cybermenaces sont souvent de nature criminelle, motivées par l'appât du gain, mais peuvent également être de nature politique et stratégique », en particulier les menaces hybrides qui se caractérisent par le déploiement de campagnes de désinformation émanant de pays tiers. Or, la volonté de l'Union de mieux gérer les actes de cybermalveillance en promouvant le développement d'une cyberdéfense européenne, notamment sur le plan de l'amélioration des capacités de l'Union, tend à devenir, à son tour, un agenda institutionnel majeur de nature à favoriser l'intensification de la lutte contre la cybercriminalité. Il convient, par conséquent, de suivre de près ce domaine prometteur sur le plan de l'intégration européenne.