NOTE STRATÉGIQUE N° 4

PARVENIR À DES POLITIQUES DE CYBERSÉCURITÉ EUROPÉENNES GLOBALES ET COHÉRENTES

Le défi : construire des politiques européennes cohérentes en matière de cybersécurité

Les politiques et réglementations de l'UE relatives à la cybersécurité manquent de cohérence, entraînant une multitude d'obligations redondantes et contradictoires.

Au cours des dernières années, l'UE a adopté de nombreuses politiques et mesures réglementaires concernant la cybersécurité. Ces dernières portaient principalement sur les domaines du marché intérieur et de la justice pénale afin de renforcer la sécurité des citoyens, des entreprises et des administrations publiques dans l'environnement numérique.

Cependant, ces **efforts souffrent souvent d'un manque de cohérence vis-à-vis des enjeux** liés aux politiques de cybersécurité. Il s'agit d'un problème qu'il convient de traiter.

La coopération directe entre les États membres de l'UE peut nuire à la protection des droits fondamentaux

Lorsqu'il s'agit d'élaborer des politiques liées à la cybersécurité, il convient de prendre des précautions pour éviter de causer des effets secondaires involontaires et néfastes, notamment en ce qui concerne la protection des droits fondamentaux des citoyens de l'Union. Dans certaines circonstances, la tâche peut s'avérer difficile. Il en fut ainsi pour la proposition de la Commission européenne de conférer aux autorités répressives un accès transfrontalier aux données (projet « e-Evidence » relatif aux preuves électroniques).

Une étude réalisée par la commission des libertés civiles, de la justice et des affaires intérieures (LIBE) du Parlement européen a analysé cette proposition. Elle a constaté que le régime de coopération accrue facilitant l'accès rapide des États membres de l'UE aux données des fournisseurs empêcherait les États « d'assumer leurs responsabilités en matière de protection efficace des droits fondamentaux sur leur territoire ». Cela engendrerait une incertitude juridique tant pour les fournisseurs de services que pour les utilisateurs.

Le phénomène est principalement lié au fait que la proposition prévoyait de transférer les responsabilités de protection des États membres de l'UE vers les fournisseurs de services et/ou les autorités compétentes, affaiblissant significativement la protection des droits fondamentaux des individus. Il semble souhaitable de traiter de ce problème dans la suite du processus législatif.

Le concept de « cybersécurité » continue à évoluer

Les documents stratégiques et les mesures législatives ne concernent souvent que certains aspects du domaine de la cyber-sécurité et sont adoptés sans être envisagés dans le cadre juridique global.

On avance souvent qu'il est difficile d'assurer une cohérence dans les politiques en matière de cybersécurité en raison des différentes manières de comprendre tant la cybersécurité, que sa portée.

De nombreuses définitions de la « cybersécurité » sont actuellement utilisées, à l'échelle de l'UE ainsi qu'au niveau national, par les institutions de l'Union, les parties prenantes et les États membres.

Les définitions de la cybersécurité varient et dépendent du destinataire, du contexte et du domaine de compétence dans lequel elles sont utilisées.

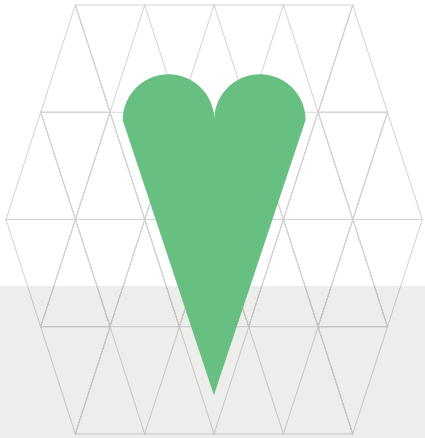
Dans le domaine de la cybersécurité au sein de l'UE, les discussions peuvent inclure divers aspects spécifiques et complexes tels que la cyber-résilience, la cybercriminalité, la cyberdéfense, la cybersécurité au sens strict, et d'autres thèmes généraux liés au cyberespace.

Les différentes significations du terme « cybersécurité » peuvent présenter des avantages et des inconvénients.

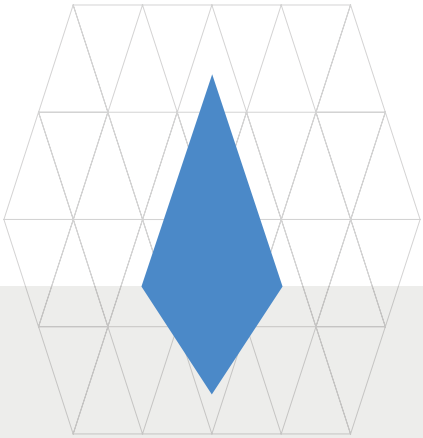
- Le terme possède la **flexibilité** nécessaire pour s'adapter à l'évolution de la situation, mais...
- ...il **crée également des frictions** entre le pouvoir de l'UE et celui des États membres, en particulier dans le domaine de la sécurité nationale.
- Par ailleurs, **il est difficile de définir la portée** d'un tel terme du fait qu'il est en constante évolution. Il peut s'appliquer à un champ excessivement large, entravant la mise en place d'une réglementation cohérente dans le domaine.
- **Il convient de lever l'ambiguïté autour du terme « cybersécurité »** afin de clarifier la fragmentation réglementaire ainsi que les responsabilités institutionnelles.

La cybersécurité possède plusieurs facettes, affectant de nombreux domaines

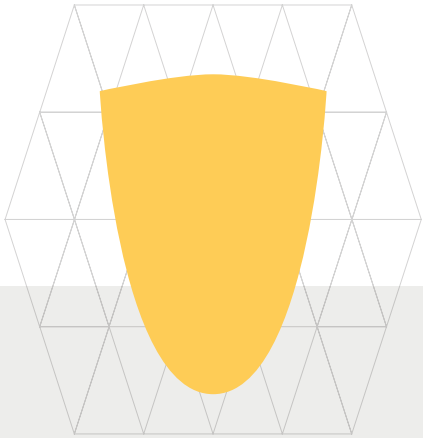
Parmi les aspects notables des domaines politiques de la cybersécurité, on peut citer la cybercriminalité, les mesures de sécurité des réseaux et de l'information, ainsi que les communications électroniques. Nombre de ces aspects ont également un impact sur le cadre européen de protection des données.



Santé



Commerce



Police et sécurité nationale

Il est d'autant plus complexe de conceptualiser la cybersécurité que **les frontières entre les différents domaines** de cette dernière **s'estompent.** Ces domaines sont liés à l'expertise professionnelle et factuelle requise, par exemple en ingénierie de sécurité, en gestion de la sécurité opérationnelle et des vulnérabilités, ou en matière de normes et cadres de sécurité informatique.

L’UE et ses États membres définissent la cybersécurité différemment

D’autres pays disposent également de définitions très variées dans leurs documents stratégiques, avec des champs d’application allant du très limité au plus général.

Par exemple, la **stratégie de cybersécurité 2013 de l’Union européenne** donne la définition suivante : « La cybersécurité fait généralement référence aux garanties et actions pouvant être utilisées afin de protéger le cyberdomaine, tant dans le domaine civil que militaire, contre les menaces à l’encontre de son infrastructure d’information et de réseaux interdépendants, ou susceptibles de lui nuire. La cybersécurité s’efforce de préserver la disponibilité et l’intégrité des réseaux et de l’infrastructure, ainsi que la confidentialité des informations qu’ils contiennent. »

En revanche, les États membres de l’UE ont élaboré, au niveau national, leur propre définition de la cybersécurité en reprenant des approches de leur pays destinées à faire face aux défis et aux menaces en matière de cybersécurité. Par exemple, la **stratégie de cybersécurité de la République tchèque** pour la période 2015–2020 stipule que « la cybersécurité comprend un ensemble de mesures et d’outils organisationnels, politiques, juridiques, techniques et pédagogiques visant à créer un cyberespace sécurisé, protégé et résilient [...] ».

On peut également citer la **Stratégie nationale de cybersécurité III adoptée par le Luxembourg en 2018**, qui stipule que la cybersécurité « est un ensemble d’outils, de politiques, de concepts de sécurité, de mécanismes de sécurité, de lignes directrices, de méthodes de gestion des risques, d’actions, de formations, de bonnes pratiques, de garanties et de technologies qui peuvent être utilisés pour protéger le cyber-environnement, son organisation et les actifs de ses utilisateurs », tout en mettant l’accent sur la disponibilité, l’intégrité et la confidentialité comme objectifs de protection.

Incertitude quant aux compétences de réglementation de l'UE en matière de cybersécurité

La difficulté liée à la création de politiques globales et cohérentes en matière de cybersécurité est encore aggravée par **l'incertitude quant aux compétences de l'UE en matière de législation sur les questions de cybersécurité**. L'UE n'a que la compétence qui lui est conférée par les États membres dans les traités. Selon les contextes et les interprétations, l'Union peut avoir une compétence exclusive, une compétence partagée ou bien encore une compétence se limitant à mener des actions de soutien, de coordination ou complémentaires.

La cybersécurité ne pouvant être exclusivement rattachée à aucun domaine politique en particulier, l'UE doit constamment chercher une **clarification des justifications juridiques pour l'adoption de mesures réglementaires en matière de cybersécurité** dans des domaines politiques bien définis.

Qui réglemente les différents domaines de la cybersécurité ?

Il convient de prendre consciencieusement en considération les questions de compétence pour aborder efficacement les dimensions internes, externes et de défense de la cybersécurité.

L'UE a appris à utiliser le terme « cybersécurité » avec beaucoup de précautions. Par exemple, on retrouve de telles précautions dans la proposition de la Commission européenne relative à la directive SRI (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). La proposition avançait que les diverses pratiques des États membres en matière de mesures de cybersécurité entravaient la protection accordée aux consommateurs et aux entreprises, réduisant ainsi « le niveau général de sécurité des réseaux et des systèmes d'information ». En d'autres termes, la Commission suggérait que des mesures de (cyber)sécurité supplémentaires étaient nécessaires.

On pourrait donc penser que l'UE a reconnu qu'il existait un **« problème de compétence »**, lequel est au cœur des relations entre l'Union et ses États membres.

Promouvoir la coopération entre les parties prenantes

La lutte contre les menaces graves à la cybersécurité doit être reconnue comme une question nécessitant l'expertise et la coopération des parties prenantes concernées dans différents domaines tels que l'informatique, la psychologie, le droit, l'éducation, le commerce et les politiques.

L'UE adopte déjà une telle approche multipartite avec la participation initiale des secteurs public et privé.

Ces parties prenantes comprennent des institutions gouvernementales, des fournisseurs d'accès Internet, des entreprises de technologie et de sécurité, des entreprises commerciales et la société civile, engagées à lutter contre les menaces à la cybersécurité.

Cependant, une telle coopération pourrait être renforcée.

Coopération institutionnelle au niveau de l'UE

Au niveau de l'UE, un certain nombre d'institutions, d'agences et de services de l'UE se concentrent déjà sur les questions de cybersécurité, telles que les directions générales de la CE (DG CONNECT, DG Mobilité et transports, et DG Centre commun de recherche, par exemple).

Compte tenu de l'importance et de la dépendance croissantes des sociétés vis-à-vis des TIC, on peut s'attendre à ce que le nombre de DG concernées par les questions de cybersécurité augmente continuellement.

Mais bien que des efforts aient déjà été déployés en vue d'établir une coopération entre les DG pertinentes et les différentes unités au sein de celles-ci, il ne s'agit souvent que de pratiques informelles. **Aucune politique officielle ne régit la coopération et les échanges** entre ces institutions.

Certaines institutions tentent de développer cette coopération par des moyens à la fois formels et informels, tels que des réseaux d'experts spécialisés, des conférences et des réunions multipartites. Toutefois, les efforts visant à établir une meilleure coopération institutionnelle se sont révélés, jusqu'à présent, incohérents, incomplets et pas particulièrement efficaces.

Les futures **initiatives politiques devraient établir une distinction claire entre les rôles, les compétences et les objectifs des domaines et acteurs concernés**. Cela est particulièrement important pour savoir si l'on doit poursuivre des stratégies de cybersécurité plutôt offensives ou plutôt défensives.

Coopération institutionnelle au niveau national

Il existe plusieurs groupes de coopération, tels que le comité européen de la protection des données ou l'Organe des régulateurs européens des communications électroniques (ORECE). Un échange de savoir-faire et d'informations entre les CERT et les autorités répressives existe au niveau national et international, mais il pourrait encore être amélioré. Par conséquent, **une action est nécessaire pour traiter le manque de personnel et l'inefficacité des institutions**, afin de réussir à impliquer suffisamment tous les acteurs concernés.

Les stratégies 2013 et 2017 de l'UE en matière de cybersécurité préconisent toutes deux une approche globale de la protection de la cybersécurité. Elles s'intéressent également aux approches nationales en matière de cybersécurité, qui ne relèvent pas uniquement de l'échelle nationale, mais aussi des interactions entre l'UE et ses États membres.

Des décisions stratégiques bien équilibrées sont nécessaires

Les thèmes controversés des débats autour du choix entre stratégie de cybersécurité offensive ou défensive incluent l'utilisation du soi-disant accès légal, le cryptage efficace sans portes dérobées (backdoors) ou les exploits « jour-zéro ».

Bien que ces mesures et outils puissent être déployées par les agences de sécurité pour combattre la criminalité, ils peuvent avoir de **graves effets secondaires collatéraux**, tel que l'affaiblissement général de la sécurité des systèmes de TIC pour tout le monde.

Lorsqu'il s'agit de traiter ces sujets, l'Union européenne doit s'efforcer de répondre sérieusement aux préoccupations relatives à l'affaiblissement potentiel de l'ensemble de l'environnement de la sécurité des technologies de l'information, de la protection de la vie privée et des données, ainsi que de la protection des droits de l'homme en général.

Pour promouvoir des politiques de cybersécurité cohérentes et axées sur les valeurs, il serait judicieux d'impliquer des experts en sécurité, des autorités de protection des données, des défenseurs des droits de l'homme ainsi que le grand public. Il est nécessaire **d'atteindre un meilleur équilibre entre les besoins en matière d'application de la loi et les droits des citoyens**.

La loi récemment adoptée sur la cybersécurité constitue un exemple de progrès, car elle clarifie au moins la structure de gouvernance en précisant les différents rôles de l'ENISA. L'ENISA consulte la CE sur les questions de cybersécurité et fournit un centre de coordination des savoir-faire, facilitant ainsi la coopération et la coordination entre les parties concernées.

Viser une cybersécurité axée sur les valeurs

Il est nécessaire de respecter les normes les plus élevées en matière d'État de droit et de protection des droits fondamentaux.

Cela est particulièrement crucial dans le domaine de l'application des lois et de la procédure pénale, ainsi que dans les cas de coopération et d'échange d'informations, où **un équilibre délicat doit être trouvé entre les intérêts des citoyens, des sociétés et des États membres**.

Bien que la plupart des États membres aient élaboré leurs premières stratégies de cybersécurité avant l'adoption de la directive SRI, celle-ci pourrait être utile pour préciser le cadre de gouvernance au niveau national, en définissant les rôles et les responsabilités des parties prenantes, tant au niveau du secteur public que privé. Ainsi, il convient d'examiner soigneusement la capacité de telles mesures législatives à s'adapter dans le contexte global.

Par conséquent, les responsables politiques doivent **acquérir une connaissance claire et précise des limites à la coopération en matière de cybersécurité imposées par les principes judiciaires et de légalité**, et s'efforcer de préserver la cohérence entre les différents cadres législatifs.

Premières étapes pour l'amélioration des politiques de cybersécurité

Mesures recommandées pour atténuer les incohérences entre les politiques européennes en matière de cybersécurité :

Garantir que les États membres fournissent toujours un niveau de protection suffisant des droits fondamentaux des personnes, notamment en ce qui concerne l'équilibre entre sécurité et protection des données à caractère personnel.

Convenir d'une définition précise et commune à l'échelle européenne du terme « cybersécurité » et des domaines d'expertise concernés lors de l'élaboration de nouvelles règlementations politiques.

Lever toute ambiguïté sur les compétences réglementaires.

Lors de l'attribution des tâches et obligations des institutions à travers les politiques, établir une distinction claire entre les rôles, les compétences et les objectifs des domaines et acteurs impliqués.

Évaluer et améliorer les pratiques d'échange d'informations.

Clarifier les relations entre les CERT publics et privés, et garantir que tous respectent les règles et directives déontologiques en matière de protection des données.

Où trouver de plus amples informations

Les diapositives sont fondées sur les travaux de recherche menés par le projet CANVAS (Création d'une alliance pour une cybersécurité axée sur les valeurs).

L'objectif du projet CANVAS est de réunir les parties prenantes des domaines clés de la stratégie numérique pour l'Europe afin de relever le défi consistant à définir les modalités d'alignement de la cybersécurité sur les valeurs européennes et les droits fondamentaux.

CANVAS fournit notamment les ressources suivantes :

- Documents d'information
- Programme de référence du projet CANVAS
- CANVAS MOOC
- Livre en libre accès
  « L'éthique de la cybersécurité »

La diapositive suivante présente nos livres blancs abordant les détails des défis de la cybersécurité.

Bibliographie : les défis de la cybersécurité (livres blancs de CANVAS)

Défis éthiques

Yaghmaei, Emad, Ibo van de Poel, Markus Christen, Bert Gordijn, Nadine Kleine, Michele Loi, Gwenyth Morgan et Karsten Weber. 2017. “Canvas White Paper 1 – Cyber-security and Ethics.” Document universitaire SSRN No 3091909. Rochester, NY: Social Science Research Network.

https://papers.ssrn.com/abstract=3091909.

Défis juridiques

Jasmontaite, Lina, Gloria González Fuster, Serge Gutwirth, Florent Wenger, David-Olivier Jaquet-Chiffelle et Eva Schlehahn. 2017. “Canvas White Paper 2 – Cybersecurity and Law.” Document universitaire SSRN No 3091939. Rochester, NY: Social Science Research Network.

https://papers.ssrn.com/abstract=3091939.

Défis technologiques

Domingo-Ferrer, Josep, Alberto Blanco, Javier Parra Arnau, Dominik Herrmann, Alexey Kirichenko, Sean Sullivan, Andrew Patel, Endre Bangerter et Reto Inversini. 2017. “Canvas White Paper 4 – Technological Challenges in Cybersecurity.” Document universitaire SSRN No 3091942. Rochester, NY: Social Science Research Network.

https://papers.ssrn.com/abstract=3091942.

Informations sur le projet

Coordination du projet et contact :
PD Dr. sc. ETH Markus Christen
Université de Zurich (UZH),
Digital Society Initiative
Rämistrasse 66, 8001 Zurich

Version du document visuel :
Version 2.0 octobre 2019

Durée du projet :
sept. 2016 – oct. 2019

Partenaires :
Le consortium CANVAS comprend 11 partenaires (9 établissements universitaires et 2 partenaires extérieurs au monde universitaire) répartis dans 7 pays européens.

Financement :
1,57 million d'euros, dont 1 million financé par la Commission européenne, la partie restante provenant du Secrétariat d'État suisse à la formation, à la recherche et à l'innovation.

Avis de financement pour CANVAS

Cofinancé par le programme Horizon 2020
de l'Union européenne

Le projet CANVAS (Création d'une alliance pour une cybersécurité axée sur les valeurs) a bénéficié d'un financement du programme de recherche et d'innovation Horizon 2020 de l'Union européenne au titre de la convention de subvention n° 700540. Ce travail a été financé (en partie) par le Secrétariat d'État suisse à la formation, à la recherche et à l'innovation (SEFRI) sous le numéro de contrat 16.0052-1. Les opinions exprimées et les arguments employés dans le présent document ne reflètent pas nécessairement les points de vue officiels de l'UE et du gouvernement suisse.