NOTRE EUROPE
Institut Jacques Delors
Thinking Europe • Penser l'Europe • Europa denken

Cybersécurité et protection des données en Europe

Menaces et perspectives

EUROPE DANS LE MONDE

DÉCRYPTAGE
MARS 2022

#défense
#digital
#sécurité

Arnault Barichella
Expert en cybersécurité

I • Les menaces associées à la cybersécurité et à la confidentialité des données en Europe

I NUMÉRISATION DES INFRASTRUCTURES CRITIQUES

Les infrastructures critiques en Europe connaissent actuellement une « révolution numérique ». La nature de cette révolution est complexe mais elle consiste essentiellement en un remplacement progressif des processus mécaniques et analogiques par des technologies numériques et des logiciels informatiques. La concurrence mondiale et les interconnexions entre les entreprises et entités des différents secteurs ont accru la pression pour accélérer la numérisation. L'obligation de rationaliser les processus de production, de consommation et de distribution, l'exigence d'un transfert rapide des informations et des données sur de longues distances, ainsi que la nécessité d'améliorer les communications internes entre les sites de gestion et les infrastructures, ont précipité cette transition. La majorité des infrastructures essentielles au fonctionnement de la société sont concernées : les secteurs vitaux tels que l'approvisionnement en eau, la santé, les transports, les communications, l'énergie, certains aspects clés de l'économie et des services, ainsi que les forces de sécurité (police/armée).

L'Europe s'appuie sur différents types de systèmes numériques, adaptés aux spécificités de chaque secteur. Ainsi, les systèmes de contrôle industriel (ICS[1]) et les systèmes de contrôle et d'acquisition de données (SCADA[2]) sont utilisés dans de nombreux domaines liés à l'industrie, ce qui permet une gestion à distance des équipements. Ils ont contribué à améliorer toute la chaîne d'approvisionnement, offrant davantage de

1 *Industrial Control Systems* – ICS.
2 *Supervisory control and data acquisition system* – SCADA.

biens et services sur mesure, l'obtention des données en temps réel par les systèmes informatiques permettant le développement de profils de consommateurs. Ces éléments ont considérablement élargi les marges de manœuvre des entreprises, augmentant ainsi leurs profits. Le secteur public a également bénéficié de ces changements, notamment grâce à l'amélioration de l'efficacité et à une meilleure rationalisation. Si elle offre de nombreux avantages, **la « révolution numérique » est cependant à double tranchant dans la mesure où elle a aussi généré de nouvelles menaces et des risques sérieux en termes de cybersécurité et de confidentialité des données.**

Ces failles sont variées et ont pris des formes différentes. Ainsi, alors que les réseaux européens étaient relativement fermés lorsqu'ils fonctionnaient selon des processus mécaniques et analogiques, les technologies numériques ont ouvert les équipements et infrastructures à l'Internet, entraînant d'importants transferts et partages de données avec des systèmes extérieurs. Il en a résulté une multiplication des opérateurs recourant à « l'Internet des objets » (IDO ou IoT[3]), qui consiste à connecter des objets ou appareils physiques à l'Internet pour procéder à des échanges de données ou pour interagir avec d'autres systèmes similaires. En outre, un certain nombre de secteurs tels que l'industrie, les transports, l'approvisionnement en eau, l'énergie et la santé dépendent souvent de cycles d'investissement à long terme : ils reposent donc potentiellement sur des infrastructures construites avant que la cybersécurité n'ait été considérée comme une menace majeure. De ce fait, l'équipement et les systèmes n'étaient souvent pas conçus pour protéger contre les cyber-attaques, mais privilégiaient plutôt la fiabilité. Cela complique également l'accès à l'historique de la configuration des infrastructures, ce qui peut rendre la modernisation de l'équipement d'autant plus difficile aujourd'hui. En outre, les caractéristiques de nombreux secteurs sont uniques, ou du moins assez spécifiques, ce qui signifie que les systèmes de cyber-protection ne peuvent souvent pas être facilement transposés d'un secteur à un autre.

Les cyber-attaques permettent aux potentiels pirates informatiques de cibler simultanément plusieurs points faibles, ce qui n'est pas le cas pour un dommage physique résultant d'une opération de sabotage par exemple. Très souvent, quelques rares failles au sein d'un système suffisent à la propagation d'un virus à l'ensemble d'un réseau. Cette situation est exacerbée par l'évolution constante et rapide des systèmes numériques due aux mises à jour fréquentes des logiciels, susceptibles de comporter des vulnérabilités « zero-day » qui, par définition, ne sont pas encore connues ou corrigées. Ces dernières constituent des failles qui n'ont pas été anticipées durant la conception d'une nouvelle technologie, et qui peuvent rester inaperçues pendant des années après la commercialisation. Il arrive aussi fréquemment que l'erreur et la négligence humaines soient responsables de l'intrusion de cyber-virus. Cela vient souvent d'un manque de formation du personnel, qui ouvre la voie au piratage informatique. L'Europe dans son ensemble est confrontée à un problème récurrent de formation inadaptée dans tous les secteurs, qu'il s'agisse des entités publiques ou privées. De ce fait, **le risque croissant d'effondrement systémique est réel, notamment en raison de la forte interconnexion entre les différents secteurs.** Par exemple, une cyber-attaque ciblant initialement l'industrie énergétique peut rapidement se propager pour contaminer d'autres secteurs clés tels que la santé, les transports, les communications, le secteur bancaire, la finance/assurance, ainsi que la défense et l'armée, mettant la société brusquement à l'arrêt.

PROFIL DES DIFFÉRENTS TYPES DE CYBER-ATTAQUES ET VIOLATIONS DE LA CONFIDENTIALITÉ DES DONNÉES

La fréquence et la sophistication des cyber-attaques ont augmenté de manière exponentielle au cours des dernières années. La révolution numérique ayant une portée très vaste, pratiquement tous les secteurs ont été impactés, même si des variations sont à noter entre les différents domaines. De plus en plus, ces attaques ciblent non seulement des entreprises privées mais

3 *Internet of Things* – IoT.

aussi des institutions publiques telles que les services ou ministères nationaux, affectant à la fois les bureaux administratifs et les infrastructures physiques, les deux étant souvent interconnectés. **Des milliers d'attaques sont rapportées chaque année en Europe, les entreprises et institutions étant désormais quotidiennement confrontées aux cyber-menaces.** Même si celles-ci prennent différentes formes, elles peuvent généralement être classées selon trois grandes catégories:

1. Interrompre l'approvisionnement ou la fourniture d'un service.

2. Endommager l'équipement en affectant l'intégralité des systèmes et/ou infrastructures.

3. Espionner pour s'approprier des informations ou données confidentielles.

Les cyber-attaques peuvent parfois combiner plusieurs de ces caractéristiques, même si la majorité des piratages répertoriés reste motivée par des considérations financières. Ces attaques font généralement usage du cyber-espionnage dans une optique d'appropriation d'informations confidentielles, souvent réalisé par des pirates informatiques appartenant à une organisation criminelle, qui cherchent ensuite à vendre les données volées sur le marché noir. Ce modèle a été exacerbé par l'essor des plateformes « big data », qui stockent de nombreuses informations personnelles grâce à des processus de sous-traitance qui ne sont pas toujours sécurisés. Dans certains cas, ces processus contournent les garanties prévues par la législation européenne sur la protection des données personnelles (voir ci-dessous). Cette tendance s'explique par une dépendance croissante à l'égard des technologies de « cloud computing » (informatique dématérialisée ou informatique en nuage), qui utilisent des serveurs internet lointains, souvent basés dans des pays hors de l'Europe, pour stocker et traiter des quantités massives de données, au lieu de recourir à des serveurs locaux ou personnels[4].

Si le cyber-espionnage à grande échelle peut être très profitable, il reste néanmoins difficile à mettre à œuvre dans la mesure où il requiert des compétences techniques avancées en informatique, ainsi que des ressources importantes pour monter l'opération sur plusieurs mois. De ce fait, les experts estiment que **certains pays influents ont sans doute soutenu un nombre croissant de cyber-attaques au cours des dernières années**, notamment au plan financier et organisationnel. **Les dynamiques géopolitiques sont désormais largement reconnues comme un facteur majeur dans un nombre croissant de cyber-attaques à travers le monde, y compris en Europe.** Si le piratage informatique motivé par des raisons géostratégiques vise souvent à interrompre ou endommager des systèmes ou équipements, le cyber-espionnage en a souvent été une motivation sous-jacente.

Compte tenu des effets potentiellement très destructeurs des **cyber-attaques, elles peuvent être considérées comme un acte de guerre.** Leur origine reste cependant très difficile à identifier en raison de l'utilisation fréquente de « fausses bannières » par les groupes de pirates. Des gouvernements peuvent ainsi lancer des cyber-assauts à grande échelle, tout en évitant de se dévoiler ouvertement. L'identification peut aussi être problématique en raison du décalage de six à sept mois en moyenne avant la découverte d'un virus ayant affecté un équipement ou un système, ce qui rend encore plus difficile le déploiement d'une réponse efficace. En outre, même si les cyber-attaques ciblent souvent des entreprises ou institutions spécifiques dans un pays donné, elles ont ensuite tendance à se propager au niveau international. Cela s'explique par la mondialisation des technologies numériques ainsi que l'interdépendance économique, les grandes entreprises possédant souvent des filiales dispersées dans plusieurs pays à travers le monde. Le tableau ci-dessous résume les caractéristiques de plusieurs des principales cyber-attaques ayant touché l'Europe au cours des dernières années :

4 Barichella A. (2019), The US-EU Rivalry for Data Protection: Energy Sector Implications, Édito Énergie, Ifri. [Titre en français : « La rivalité entre les États-Unis et l'Europe pour la protection des données : conséquences pour le secteur énergétique » ; résumé en français ici ; article complet disponible uniquement en anglais]

Year	Nom	Cible	Conséquences	Objectif	Assaillant
2015	*Black Energy*	Réseau électrique ukrainien	• Plus de 30 opérateurs électriques déconnectés du réseau pendant plusieurs heures. • Plus de 200 000 personnes impactées. • Propagation à plusieurs pays de l'UE ayant des liens commerciaux avec l'Ukraine.	• Interruption de l'approvisionnement • Endommagement de l'équipement	• Russie soupçonnée
2017	*NotPetya*	Infrastructures critiques et réseaux informatiques en Ukraine	• 30% de l'ensemble des systèmes informatiques ukrainiens contaminés. • Dommages estimés à 10 milliards $. • Un million de personnes affectées (dans les banques, les ministères nationaux, les opérateurs électriques, les journaux, etc.).	• Interruption de l'approvisionnement • Endommagement des équipements • Espionnage potentiel	• Russie soupçonnée
2017	*WannaCry*	Attaque mondiale affectant plus de 150 pays (y compris la majorité des États membres de l'UE)	• Cyber-attaque mondiale sans précédent. • Utilisation du cryptage des données pour réclamer le paiement de rançons. • Diversité des secteurs affectés : Service de santé britannique (NHS), Chemins de fer fédéraux allemands, constructeur automobile français Renault, laboratoires informatiques d'universités italiennes, entreprises de télécommunications et d'énergie en Espagne et au Portugal. • Dommages estimés à plusieurs milliards $.	• Espionnage • Demande de rançon	• Corée du Nord soupçonnée
2022	*Wiper + Déni de service distribué (DDOS[5])*	Infrastructures critiques ukrainiennes, système bancaire, sites militaires et gouvernementaux	• Objectif de fermeture de sites internet et d'effacement des données des équipements contaminés, en submergeant les systèmes avec des volumes massifs de demandes. • Cyber-attaques régulières à grande échelle pour déstabiliser l'Ukraine avant et pendant l'invasion russe. • « Guerre hybride » : cyber-attaques + attaques militaires conventionnelles. • Risque de propagation aux États voisins membres de l'UE.	• Interruption de l'approvisionnement • Endommagement des équipements • Espionnage potentiel	• Russie

5 *Distributed Denial of Service* – DDOS.

II • Perspectives sur les politiques de cybersécurité et de protection des données en Europe

L'APPROCHE « GLOBALE » DE L'UE EN MATIÈRE DE CYBERSÉCURITÉ, DE PROTECTION DES DONNÉES ET D'INTELLIGENCE ARTIFICIELLE

Face aux menaces et risques croissants en termes de cybersécurité liés à l'accélération de la « révolution numérique », l'UE a progressivement mis en place un certain nombre de politiques et législations majeures au cours des dernières années. Au fil du temps, elles ont évolué pour constituer une approche distincte, qui peut être définie à la fois comme étant « globale » et « souple »[6]. Le volet « global » tient à l'ambition de l'UE de s'attaquer simultanément à de nombreux aspects différents en lien avec la cybersécurité. Cela inclut notamment les infrastructures critiques en général, en s'intéressant à la fois à la sécurité et à la protection des données, tout en accordant aussi une attention croissante au nouveau domaine de l'intelligence artificielle, ainsi qu'aux liens potentiels avec la transition énergétique.

Pour commencer, la législation européenne sur la protection des données reflète cette dimension « globale ». Le règlement général relatif à la protection des données (RGPD), adopté en 2016 et en vigueur depuis 2018, a remplacé la directive de 1995 sur la protection des données. Son importance tient au fait qu'il vise à couvrir à la fois « la protection des données » (en limitant l'appropriation injustifiée des données personnelles) et la « sécurité des données » (règles sur la gestion du traitement des données une fois collectées). Le RGPD représente l'une des initiatives législatives les plus avancées au monde dans ce domaine, avec des clauses exhaustives et strictement appliquées, prévoyant en cas de non-respect des sanctions pouvant aller jusqu'à 20 millions € ou 4 % du chiffre d'affaires annuel pour les entreprises.

Ensuite, la Commission européenne a récemment fait part de son intention de développer une approche européenne concernant l'intelligence artificielle. La Commission adoptera un cadre axé sur l'évaluation des risques et reposant sur les deux piliers que sont l'excellence et la confiance, de manière à stimuler la recherche et la capacité industrielle, tout en garantissant la protection des droits fondamentaux. L'UE a souligné qu'une Europe résiliente prête pour la « décennie numérique » est une Europe dans laquelle les citoyens et les entreprises peuvent bénéficier des progrès générés par l'intelligence artificielle, applicables à la fois pour l'industrie et la vie quotidienne. La dimension globale apparaît dans la proposition de règlement faite en 2021 visant à établir un cadre règlementaire européen commun sur l'intelligence artificielle, qui s'appliquerait à tous les secteurs (excepté le domaine militaire), ainsi qu'à tous les types d'intelligence artificielle. Cette proposition législative définit quatre catégories pour la régulation de l'intelligence artificielle, allant de la catégorie « interdite » à celle de « risque faible». Cela inclut la mise en place d'un système d'enregistrement à l'échelle européenne pour les algorithmes d'intelligence artificielle, ainsi qu'une procédure de surveillance destinée aux secteurs susceptibles de s'exposer à des risques en cas de recours à l'intelligence artificielle, tels que l'énergie ou la santé.

Troisièmement, alors que l'accélération de la numérisation de l'industrie énergétique a apporté de nombreux avantages, elle a aussi considérablement accru les risques en termes de cybersécurité au sein de ce secteur hautement stratégique, en partie du fait de l'essor des réseaux intelligents et du déploiement à grande échelle des compteurs communicants. Au cours des dernières années, en cohérence avec sa dimension « globale », **la législation européenne sur l'énergie propre a systématiquement cherché à inclure un volet cybersécurité**, à commencer par le paquet législatif « Une énergie propre pour tous les Européens » annoncé en 2016. Il en a résulté une révision du règlement européen sur le marché intérieur de l'électricité en 2019, qui a permis le développement d'un code de réseau en matière de cybersécurité pour le secteur de l'électricité, et dont une partie se concentre sur les énergies renouvelables. Un groupe de travail sur les réseaux intelligents (*smart*

6 Barichella A. (2018), Cybersécurité des infrastructures énergétiques : regards croisés Europe/États-Unis, Études de l'Ifri, Ifri.

grids task force) a été créé en 2017 pour préparer ce code de réseau, tandis que le Pacte vert pour l'Europe comporte également des dispositions pour améliorer et renforcer ce code.

Quatrièmement, pour ce qui est des infrastructures critiques en général, la législation et les politiques européennes remontent au programme européen de protection des infrastructures critiques de 2006, ainsi qu'à la directive de 2008 sur les infrastructures critiques, qui fixent aux États membres des lignes directrices assez souples et générales. Plus récemment, la directive de 2016 sur la sécurité des réseaux et des systèmes d'information (NIS[7]) est devenue le principal cadre législatif dans ce domaine. Cette directive a contribué au développement de normes européennes communes pour la cybersécurité des « opérateurs de services essentiels », qui incluent un large éventail d'infrastructures considérées comme étant essentielles au bon fonctionnement de la société. Dans le prolongement de cette directive, la loi européenne sur la cybersécurité (*EU Cybersecurity Act*) finalisée en 2019 définit des procédures renforcées pour l'adoption de la directive NIS, tout en lançant un système de certification à l'échelle européenne pour une large gamme de produits et services numériques, avec l'objectif de créer un **marché intérieur pour la cybersécurité**.

SOUPLESSE DANS L'APPROCHE DE L'UE : DES PARADIGMES NATIONAUX DIFFÉRENCIÉS À VITESSE VARIÉE

Si les avantages du volet « global » de l'approche de l'UE sont apparents en matière de cybersécurité, on ne peut pas en dire autant de sa « souplesse ». En effet, dans la plupart des cas, les États membres se sont vus octroyés une large marge de manœuvre et un degré d'autonomie important concernant la mise en œuvre des normes européennes. Ainsi, pour la directive NIS, chaque État membre est chargé du développement de sa propre stratégie nationale de cybersécurité. Bien qu'une stratégie européenne de cybersécurité ait été définie en 2013 et révisée en 2020, elle se contente de fournir des recommandations générales, laissant aux États membres la tâche de définir les détails au niveau national. Cela vaut également pour l'entité régulatrice régionale dans ce domaine, initialement connue sous l'appellation ENISA[8], mais qui est désormais désignée comme l'Agence de l'Union européenne pour la cybersécurité. La loi de 2019 sur la cybersécurité lui a octroyé un mandat permanent et un budget accru, ainsi que de nouveaux outils pour soutenir les pays dans leur mise en œuvre de la directive NIS. Si la portée de l'ENISA est globale dans la mesure où elle s'occupe de tous les secteurs, ses compétences restent limitées car elle vise essentiellement à agréger et diffuser des données, fournir des conseils aux États membres et encourager la collaboration. De ce fait, elle manque de tout cadre contraignant pour parvenir à la mise en conformité avec les normes européennes.

Cela apparaît aussi dans l'obligation imposée par la directive NIS que chaque État membre mette en place une équipe d'intervention en cas d'incident lié à la sécurité informatique (CSIRT[9]). Toutes ces équipes nationales ont été rassemblées au sein d'un réseau européen commun, en parallèle de la création d'un « groupe de coopération » incluant la Commission européenne et les cyber-agences des États membres. Cependant, comme avec l'ENISA, ces cadres ne disposent pas des compétences nécessaires, telles que les sanctions, pour assurer la mise en conformité avec les normes à l'échelle européenne. Cette responsabilité est en revanche attribuée aux autorités des États membres, qui sont libres de déterminer le degré d'autorité qu'elles souhaitent attribuer à leur équipe d'intervention CSIRT au niveau national. Cela a conduit à l'émergence de **disparités importantes, avec un paradigme marqué par de fortes différenciations en termes de l'efficacité des équipes CSIRT entre les pays européens.** On peut dresser un état des lieux similaire dans des secteurs plus spécialisés tels que celui de l'énergie. Ainsi, le règlement de 2019 sur la préparation aux risques dans le secteur de l'électricité vise à établir une approche européenne pour faire face à différents types de menaces, y com-

7 *Directive on the Security of Network and Information Systems* – NIS.
8 *European Network and Information Security Agency* – ENISA.
9 *Computer Security Incident Response Team* – CSIRT.

pris la cybersécurité. Cependant, les États membres sont une fois encore libres d'élaborer leurs propres normes par le biais de plans nationaux de préparation aux risques, qui ne sont que faiblement coordonnés par un groupe sur l'électricité au niveau de l'UE. Bien que les détails de la loi sur l'intelligence artificielle n'aient pas été entièrement dévoilés, il semble néanmoins que la proposition législative octroiera une large marge de manœuvre aux États membres dans la mise en œuvre des normes de l'UE.

Pour ces raisons, **la « souplesse » de l'approche européenne a conduit à l'émergence d'un paradigme à plusieurs vitesses, où l'efficacité des cadres nationaux sur la cybersécurité est extrêmement variable d'un pays à un autre**. L'ampleur de l'autonomie accordée aux États membres a permis aux pays disposant de moyens financiers et logistiques suffisants, ainsi que des infrastructures et de l'expertise technique requises, de développer au niveau national des structures avancées en matière de cybersécurité. Cela vaut non seulement pour les États membres les plus influents et les plus peuplés comme la France et l'Allemagne, mais aussi plusieurs autres pays d'Europe du Nord, qui sont régulièrement allés plus loin que les normes européennes dans ce domaine. Ainsi, l'Agence nationale de la sécurité des systèmes d'information (ANSSI), créée en France en 2009, est généralement considérée comme l'une des plus développées non seulement dans l'UE, mais aussi à l'échelle mondiale. Elle dispose de compétences étendues pour mettre en œuvre des règles nationales de cybersécurité rigoureuses. Celles-ci reposent sur une loi de programmation militaire, initialement adoptée en 2016 puis actualisée en 2018 afin de couvrir la période 2019-2025. Cette loi établit des normes strictes et contraignantes pour la cybersécurité de plus de 200 « opérateurs d'importance vitale ». Elle a été complétée en 2016 par des arrêtés sectoriels, faisant de la France le premier pays à établir des obligations détaillées spécialement adaptées aux caractéristiques des différents secteurs, tels que le gaz et les hydrocarbures, l'électricité ou le nucléaire.

Cependant, plusieurs autres États membres ne disposent pas des ressources, de l'expertise ou des infrastructures adaptées pour développer des structures aussi avancées en termes de cybersécurité. Ainsi, des pays tels que la Bulgarie, la Grèce et la Slovaquie ont tardé à présenter une stratégie nationale de cybersécurité et à mettre en place leur équipe CSIRT, tandis que d'autres comme le Portugal, la Croatie et la Lettonie ont été critiqués pour n'avoir toujours pas élaboré de cadre adéquat pour la cybersécurité des infrastructures critiques[10]. Cette situation d'une Europe à plusieurs vitesses n'est pas sans rappeler d'autres domaines politiques, tels que Schengen ou l'euro. Cela est néanmoins particulièrement problématique pour le sujet de la cybersécurité compte tenu du degré élevé d'interconnexion entre les États membres, en lien avec les règles du marché unique et du cadre juridique pour le processus d'intégration de l'UE. De ce fait, **les pays ayant les normes de cybersécurité les moins développées constituent des maillons faibles** susceptibles de permettre aux cybervirus d'infiltrer le réseau européen, avant de se propager aux autres États membres et d'infecter potentiellement l'ensemble du système. C'est précisément ce qui s'est produit lors d'un certain nombre de cyber-attaques au cours des dernières années, comme le montre le tableau ci-dessus.

L'un des principaux obstacles à une meilleure harmonisation des normes de cybersécurité en Europe tient au fait que **les États membres hésitent à partager des informations classifiées avec leurs voisins**, et sont globalement réticents à tout transfert supplémentaire de compétences aux institutions européennes, surtout en matière de défense. Cela explique pourquoi la mise en œuvre de la directive NIS a été problématique, entraînant une fragmentation à différents niveaux sur le marché unique. En réaction, **la Commission a présenté en décembre 2021 une proposition pour une deuxième directive NIS actualisée**. Celle-ci vise à renforcer les exigences en matière de cybersécurité, à s'occuper de la sécurité des chaînes d'approvisionnement, à consolider les obligations de rapportage et à améliorer les processus de supervision et de mise en œuvre, y compris en adoptant

10 Barichella (2018).

des sanctions plus harmonisées entre les États membres. La proposition NIS2 cherche également à élargir la portée de la directive initiale en intégrant davantage d'entités et de nouveaux secteurs, l'objectif étant une harmonisation avec les secteurs couverts par les normes européennes relatives à la protection des infrastructures physiques[11].

S'il ne fait aucun doute que la directive NIS2 devrait constituer une véritable avancée, la législation pourrait s'avérer insuffisante, notamment en ce qui concerne le problème des maillons faibles. En effet, malgré l'harmonisation proposée des sanctions, les États membres resteraient chargés de définir les obligations détaillées de leurs propres cadres nationaux pour la cybersécurité, perpétuant ainsi l'enjeu de la différenciation des normes à travers l'UE. Une solution pour améliorer l'harmonisation des cyber-normes serait de **renforcer les liens entre la législation européenne dans ce domaine et la politique européenne de sécurité et de défense commune (PSDC)**. Cela pourrait contribuer à encourager un meilleur partage d'informations entre les États membres. Afin de pallier le problème des maillons faibles, la collaboration entre les pays européens et les États-Unis en matière de cybersécurité pourrait ainsi être renforcée, notamment dans le cadre de l'OTAN, qui organise chaque année un cyber-exercice appelé « *Locked Shields* ».

De façon générale, compte tenu de l'accélération de la « révolution numérique », ainsi que de l'augmentation exponentielle du nombre et de la sophistication des cyber-attaques touchant pratiquement tous les secteurs, le renforcement des politiques et de la législation de l'UE dans ce domaine devrait constituer une priorité absolue pour les décideurs européens. L'escalade de la situation en Ukraine en souligne davantage encore l'importance. En effet, des cyber-attaques à grande échelle ont été lancées au cours des mois et semaines précédant l'invasion russe afin de déstabiliser le pays, ciblant les infrastructures critiques, le système bancaire, ainsi que les sites militaires et gouvernementaux. Cela inclut des attaques de type « *wiper* » et de « déni de service distribué » (DDOS – voir le tableau ci-dessus). En raison de l'interconnexion numérique, le risque de propagation aux États voisins au sein de l'UE est réel[12]. L'armée russe a régulièrement eu recours à des techniques de « **guerre hybride** », combinant les cyber-attaques et les activités militaires conventionnelles en Ukraine, comme cela avait été le cas lors des incursions en Géorgie (2008) et en Crimée (2014). •

11 Parallèlement, la Commission a introduit une autre proposition pour une nouvelle directive sur la résilience des entités critiques, qui pourrait se concentrer sur le renforcement des normes européennes en matière de protection physique des infrastructures (ce qui diffère de la cybersécurité, couverte par la directive NIS). L'objectif consisterait à harmoniser les secteurs couverts par ces deux directives, notamment les suivants : énergie, transports, banques, marchés financiers, santé, eau potable, eaux usées, infrastructures numériques et l'espace.

12 En réponse, l'UE a annoncé le lancement d'une cyber-équipe d'intervention rapide (*cyber rapid-response team* – CRRT) constituée de cyber-experts et devant être déployée dans toute l'Europe. Celle-ci inclut des volontaires de six États membres (Lituanie, Pays-Bas, Pologne, Estonie, Roumanie et Croatie) afin d'aider l'Ukraine à se défendre contre les cyber-attaques.

Directeur de la publication : Sébastien Maillard •
 Traduction de l'anglais : Mathilde Durand • Edition : Anne-Julia Manaranche •

Institut Jacques Delors
Penser l'Europe • Thinking Europe • Europa Denken
18 rue de Londres 75009 Paris, France • www.delorsinstitute.eu
T +33 (0)1 44 58 97 97 • info@delorsinstitute.eu