CONFRONTATIONS EUROPE

Quelle stratégie pour l'UE en matière de cybersécurité ?

Arnault Barichella

PRÉSENTATION

Arnault Barichella, doctorant au Centre d'études européennes et de politique comparée de Sciences Po, est revenu dans un entretien accordé à Pierre Fouquet, chargé de missions numérique et énergie au bureau bruxellois de Confrontations Europe, sur l'importance d'une approche européenne coordonnée en matière de cybersécurité.

Pierre Fouquet : Quels sont aujourd'hui les différents types de menaces cyber pour l'UE ? Comment les Etats membres et l'Union européenne luttent-ils contre ces menaces ?

Arnault Barichella : On assiste à une révolution numérique qui impacte pratiquement tous les secteurs d'activité de l'économie européenne, y compris les plus vitaux comme l'énergie, la santé, les transports/communications, le secteur bancaire et la finance, l'armée, la police et même l'approvisionnement en eau. Cette révolution numérique est systémique car pratiquement aucun aspect de la société n'est épargné, ouvrant la porte à toute sorte de menaces. Au cours des vingt dernières années, les infrastructures de type analogique ont été progressivement remplacées par des technologies et des infrastructures numériques, passant de réseaux fermés à une configuration ouverte sur l'internet.

Même si cela a pu apporter de nombreux bénéfices, notamment économiques avec des gains d'efficacité, la révolution numérique a également introduit un nouveau type de menace lié à la cybersécurité. Celle-ci représente une menace complexe, étant donné que chaque secteur possède ses propres spécificités. Ainsi, les systèmes de cyber protection ne sont pas facilement transposables d'un secteur à l'autre.

Les Etats membres de l'UE ont progressivement fait des efforts pour mettre en place des politiques afin de se protéger face aux risques croissants en matière de cybersécurité. Des solutions efficaces peuvent résulter de l'investissement, de l'ingénierie et des infrastructures disponibles. Or, chaque pays dispose de moyens différenciés. Alors que la France ou l'Allemagne sont souvent considérés comme des leaders dans le domaine de la cybersécurité, d'autres Etats membres n'ont pas eu les mêmes moyens pour mettre en place des politiques aussi ambitieuses. Ainsi, on assiste à l'émergence d'une Europe à plusieurs vitesses, ce qui est un véritable problème.

Cela est en partie lié au fait que même si l'UE a promulgué un certain nombre de régulations au cours des dernières années avec l'objectif d'établir des normes communes en matière de cybersécurité, l'approche européenne demeure « souple » dans la mesure où elle donne aux États membres une grande marge de manœuvre dans la mise en application de ces normes. Par exemple, la directive sur la sécurité des réseaux et des systèmes d'information (NIS), adoptée en 2016 et qui sera mise à jour d'ici la fin de l'année avec la directive NIS 2, ainsi que le *EU Cybersecurity Act* adopté en 2019, ont permis le développement de normes européennes communes pour la cybersécurité des « opérateurs de services essentiels ». Malgré cela, les États membres ont conservé une marge de manœuvre et une autonomie importante concernant la transcription des normes européennes. Par exemple, en ce qui concerne la directive NIS, chaque État membre est chargé du développement de sa propre stratégie nationale de cybersécurité. Cela a eu pour conséquence l'émergence d'un paradigme différencié entre les pays de l'UE, avec une fragmentation générant des maillons faibles qui constituent potentiellement des portes d'entrée pour la propagation de virus à l'ensemble du réseau européen.

C'est pourquoi la priorité serait, selon moi, de renforcer les normes communes de cybersécurité au niveau de l'UE, notamment au travers de la directive NIS 2, en cours de finalisation. Malgré

cela, il est important de souligner que l'approche européenne en matière de cybersécurité possède également certains avantages. En effet, elle peut être qualifié de « globale », dans la mesure où elle inclut un large éventail de différents domaines. Cela comprend par exemple toutes les infrastructures critiques, la sécurité et à la protection des données à caractère personnel, une attention particulière au domaine émergent de l'intelligence artificielle, ainsi qu'aux liens entre cybersécurité et transition énergétique.

PF : Quelques jours avant l'invasion de l'Ukraine par la Russie, un groupe de pirates russes a mené une série de cyberattaques visant les sites Web du gouvernement ukrainien, des banques, de la défense et de l'aviation civile, ainsi que des systèmes d'information lettons et lituaniens ayant des liens particuliers avec le gouvernement ukrainien. Comment l'UE et les États membres peuvent-ils s'armer pour répondre aux attaques de la Russie ? Y a-t-il un changement de paradigme dans la manière de « faire la guerre », ou accélère-t-elle des tendances déjà en place ?

AB : La Russie s'est effectivement servie de cyber-attaques de grande ampleur au cours des années et des mois qui ont précédé l'invasion de l'Ukraine afin de déstabiliser le pays. Depuis l'annexion de la Crimée, la Russie organise de manière régulière ce type d'attaque contre l'Ukraine, avec notamment des cyberattaques majeures en 2015 (*Black Energy*) et 2017 (*NotPetya*). Les attaques de 2022 ont ciblé les infrastructures critiques, notamment le secteur bancaire, ainsi que des sites militaires et gouvernementaux. Pour citer quelques exemples, il y a eu des attaques de type *Wiper* ou *Distributed Denial of Service*, dont l'objectif a été la fermeture de sites internet et l'effacement des données contaminées en submergeant les systèmes avec des volumes massifs de demandes. Les cyber-attaques ayant continué pendant l'invasion, on peut qualifier cette guerre « d'hybride », dans la mesure où les offensives cyber sont combinées avec des attaques militaires de type conventionnel. L'objectif est triple : l'interruption des chaînes d'approvisionnement, l'endommagement des équipements militaires et civils, ainsi que l'espionnage. La Russie a déjà eu recours à ce type de « guerre hybride » lors des incursions en Géorgie en 2008 ou en Crimée en 2014, même si aujourd'hui l'échelle est bien plus importante.

Pour l'Europe, la menace est réelle en raison de l'interconnexion des infrastructures critiques et du risque de propagation aux États membres de l'UE. Il faut noter cependant que les cyberattaques sont moins virulentes que prévues depuis le début de l'invasion russe, tout du moins pour le moment. En outre, il semble que la Russie ait été prise de court non seulement par la résistance ukrainienne, mais également par l'unité et la fermeté des sanctions occidentales. Cela explique pourquoi les cyberattaques demeurent localisées principalement en Ukraine, du moins pour le moment. Néanmoins, le président américain Joe Biden a mis en garde sur l'éventualité de cyberattaques russes de plus grande ampleur pour déstabiliser les pays occidentaux au cours des mois et années qui viennent, ciblant notamment les infrastructures critiques.

La guerre en Ukraine a poussé les européens à renforcer en urgence leur stratégie commune en matière de cybersécurité. Par exemple, l'UE a annoncé la création d'une cyber-équipe d'intervention rapide (*cyber rapid-response team*) constituée d'experts et devant être déployée

dans toute l'Europe. Cette équipe inclut des volontaires de six États membres (Lituanie, Pays-Bas, Pologne, Estonie, Roumanie et Croatie), dont l'objectif est non seulement de protéger l'UE, mais également d'aider l'Ukraine à se défendre. Plus généralement, cette guerre semble marquer le début d'une prise de conscience qui pourrait ouvrir la porte à une Europe de la défense renforcée dans un avenir proche, notamment en matière de cybersécurité.

PF : L'espace numérique ne connait pas de frontières : L'UE peut-elle réussir seule à protéger ses entreprises et ses citoyens face au risque cyber ou faut-il réguler le secteur au niveau international ? La cybersécurité rebat-elle les cartes de la puissance dans le sens où des pays peu équipés en armement conventionnel peuvent jouer un rôle important dans le champ cyber ?

AB : Etant donné que la cybersécurité est une menace mondiale et multiforme, l'Europe ne peut pas se protéger complétement à elle seule. Par exemple, le virus « *Wannacry* » en 2017 fut une attaque mondiale sans précédent affectant plus de 150 pays dans le monde, y compris la majorité des Etats membres de l'UE, touchant une multitude de secteurs différents, avec l'utilisation du cryptage des données pour demander des rançons.

Les instances de l'ONU jouent un rôle dans la mise en place de recommandations et de normes internationales non-contraignantes dans le domaine de la cybersécurité. Néanmoins, ce type de collaboration mondiale reste problématique car elle implique de coopérer avec des pays tels que la Russie, la Chine ou l'Iran, qui sont derrière la majorité des cyberattaques ciblant l'occident.

Ainsi, et surtout dans le contexte actuel de la guerre en Ukraine, l'une des priorités devrait être de renforcer la collaboration transatlantique entre l'Europe et les Etats-Unis. Au cours des derniers mois, le conflit en Ukraine a joué un rôle majeur dans le renforcement de l'OTAN avec une solidarité occidentale historique. L'OTAN organise déjà chaque année un exercice de cybersécurité de grande ampleur dénommé « *Locked Shields Cyber Exercise* ». Ce type d'exercice constitue un moyen essentiel pour renforcer la collaboration transatlantique dans le domaine de la cybersécurité.

En outre, il serait utile de renforcer également la coopération au niveau bilatérale dans ce domaine. Il existe déjà un certain nombre de groupes de travail UE-USA qui pourraient être renforcés, notamment le dialogue UE/États-Unis sur le cyberespace depuis 2014, le groupe de travail UE/États-Unis sur la cybersécurité et la cybercriminalité depuis 2010, ainsi que le *Information Society Dialogue* depuis 2002. Au niveau du G7, on assiste également à plus de focalisation sur les thématiques en lien avec le cyber au cours des dernières années, avec la création de groupes de travail spécialisés tels que le *G7 Cyber Expert Group*.

Globalement, un autre facteur majeur qui complique davantage tout type de réponse efficace face aux cyberattaques est la difficulté d'attribution. En effet, l'utilisation de « fausses bannières » est très courante, et il est souvent ardu de déterminer avec certitude la provenance de ce type d'attaque, permettant à un pays de mener des cyber assauts de grande ampleur, sans se révéler ouvertement. Cela permet notamment à des petits pays moins bien équipés en armement conventionnel, tels que la

Corée du Nord, de jouer un rôle important dans le champ cyber, comme démontré avec le virus « *Wannacry* » en 2017, où Pyongyang est suspecté. Pour ces raisons, on peut dire que la cybersécurité rebat les cartes de la géopolitique de plusieurs manières notables.

PF : Afin de construire une industrie numérique souveraine, 22 entreprises et instituts français et allemands ont lancé le projet Gaia-X avec l'ambition de définir un cadre et des règles communes en matière de stockage de données. A plus long terme, le projet a pour but d'offrir une alternative aux infrastructures américaines et chinoises. Depuis sa naissance en 2019, le projet Gaia-X connait son lot de critiques, notamment du fait de son ouverture aux entreprises extra-européennes. Que peut-on attendre de cette initiative ?

AB : Ce projet part d'une bonne intention : contrer la prédominance américaine et chinoise dans le domaine du *Cloud Computing*. Comme le secteur n'est pas suffisamment développé en Europe, un nombre important d'entreprises européennes sont obligées d'avoir recours à des entreprises étrangères, surtout en provenance des Etats-Unis, et également de Chine dans une moindre mesure. En 2018, sous l'administration Trump, une loi controversée a été approuvée par le Congrès américain : *le Cloud Act*. Cette loi est complexe, impliquant principalement la mise en place de règles plus souples concernant le stockage des données par les entreprises américaines utilisant le *Cloud Computing*. Elle permet aux instances de justice américaines de contraindre les entreprises installées aux Etats-Unis fournisseuses de services Cloud, par mandat ou assignation, à pourvoir des données relatives aux communications électroniques, stockées dans leurs serveurs, qu'ils soient situés aux Etats-Unis ou dans des pays étrangers. Cela inclut les communications personnelles des individus, sans que ceux-ci n'en soient informés, contournant ainsi les dispositions politiques et juridiques des pays concernés. Pour ces raisons, le *Cloud Act* est problématique car il a eu pour conséquence de neutraliser un certain nombre de protections pour les données à caractère personnel établies par la législation européenne, en particulier le Règlement Général sur la Protection des Données (RGPD).

Ainsi, l'un des principaux objectifs du projet Gaia-X est de contrer la prédominance américaine dans le domaine du *Cloud Computing*, en mettant en place un serveur européen de grande ampleur dans ce domaine. Le but est donc de renforcer le RGPD non seulement face au *Cloud Act* américain, mais aussi face aux soupçons d'espionnage en provenance des entreprises chinoises sur le secteur. Néanmoins, il semblerait que l'UE ait subi certaines pressions de la part de lobby étrangers. Ainsi, la manière dont le projet Gaia-X est en train d'être mis en place a permis l'association d'un certain nombre d'entreprises américaines et chinoises dominantes sur le marché tels que Microsoft, Google ou Amazon, ainsi qu'Alibaba et Huawei. Cela va clairement à l'encontre de l'objectif principal de créer un service Cloud européen indépendant. Les compromis réalisés par l'Europe, probablement pour des raisons économiques, risquent à nouveau de rendre l'UE vulnérable en ce qui concerne la protection des données à caractère personnel des citoyens européens, fragilisant davantage le RGPD.

PF : Est-ce que l'on a bien intégré aujourd'hui tous les enjeux du cyber ? Assiste-t-on à un changement de mentalités sur ce sujet ?

AB : Je pense que ce n'est qu'en partie le cas. D'un côté, il est indéniable qu'une véritable prise de conscience sur l'importance majeure des enjeux de cybersécurité est apparue au cours des dernières années. Le conflit en Ukraine n'a fait que renforcer cette tendance au cours des derniers mois. En plus d'une prise de conscience progressive, nous avons assisté à un sursaut en France et au niveau européen pendant ces derniers mois avec un certain nombre de mesures importantes qui ont été annoncées pour renforcer les protections dans ce secteur clé. Cela inclut par exemple le lancement du nouveau campus « Cybersécurité français », inauguré à la Défense en septembre dernier, dont l'objectif est de rassembler les principaux acteurs nationaux et internationaux dans ce domaine. Il permettra en particulier d'accueillir sur un même site des entreprises, des services de l'État, des organismes de la formation, des acteurs de la recherche et des associations, avec la mise en place d'actions visant à fédérer la communauté de la cybersécurité et à développer des synergies entre ces différents acteurs.

Cependant, malgré cette prise de conscience au cours des dernières années, il est important de souligner que l'erreur et la négligence humaine demeurent un facteur majeur derrière un grand nombre de cyber-attaques. En effet, le manque de formation du personnel, tant au niveau des entreprises que des gouvernements, continue d'être un problème important en France, en Europe et dans le monde. Ainsi, des mesures adéquates pour la cybersécurité ne sont souvent pas mises en place ou le sont de manière insuffisante, ce qui a souvent eu pour conséquence de permettre l'intrusion de virus dans les systèmes informatiques. Cela est exacerbé par le fait que les entreprises et les gouvernements sont souvent réticents à déclarer les incidents cyber, par souci pour leur réputation. Ces derniers sont de plus en plus victimes de cyberattaques, ce qui représente maintenant une menace quotidienne, avec des milliers d'attaques recensées chaque année. Pour ces raisons, il est indispensable de prendre des mesures pour renforcer la formation du personnel dans les années qui viennent, non seulement en France mais également au niveau européen.

CONFRONTATIONS EUROPE

Confrontations - Paris
29 avenue de Villiers
75017 Paris

Confrontations - Bruxelles
Rue du Luxembourg 19
1000 Bruxelles

communication@confrontations.org

https//:confrontations.org

@confrontations

@ConfrontationsEurope