LES PUBLICATIONS

LA CYBER-COOPÉRATION EUROPÉENNE

Par Rémi RAVEL

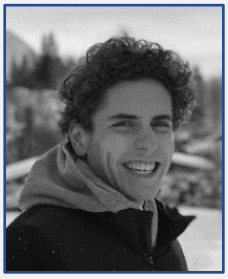
LES JEUNES IHEDN

À PROPOS DE L'ARTICLE

Les attaques cyber deviennent un moyen d'action récurrent pour déstabiliser des institutions ou des États. L'évolution de la technologie et le monde connecté qui en découle rendent ces attaques de plus en plus dommageables et dangereuses pour l'économie mais également la souveraineté des États. D'autant que ces attaques peuvent être d'une ampleur considérable comme le montrent les virus NotPetya et Wannacry de 2017 affectant des centaines de milliers d'ordinateurs du monde entier.

Jusque récemment, l'Union Européenne s'est reposée sur une politique de défense propre à chaque État avec une assurance de la protection de l'OTAN. Elle commence à se rendre compte de l'importance d'une action directe et met en place des initiatives pour coopérer entre États. Toutefois, il n'est pas certain que cela suffise pour disposer d'une véritable force cyber européenne.

À PROPOS DE L'AUTEUR



Rémi RAVEL est en Master 1 de droit public après avoir été diplomé d'une licence d'informatique et d'une licence de droit. Il s'intéresse particulièrement aux questions de coopération de défense ainsi qu'aux questions de cyber-sécurité. Il est membre du comité Europe des Jeunes IHEDN.

Introduction

« Les crises cyber ne connaissent pas de frontières » explique M. Juhan LEPASSAAR, directeur de l'ENISA. L'Union Européenne est un espace ouvert au sein duquel les biens et services peuvent circuler librement. Les logiciels et les données sont donc transmissibles très facilement au sein de l'UE impliquant une plus grande vulnérabilité aux attaques extérieures. Un virus apparaissant en Pologne peut se retrouver quelques minutes plus tard en Irlande sans passer aucune barrière de protection.

L'agence européenne chargée de la sécurité des réseaux et de l'information, ici sous l'acronyme anglais communément utilisé ENISA est l'agence européenne de cyber sécurité créée en 2004. L'objectif originel de cette agence est l'analyse et l'évaluation des méthodes de chaque pays dans la cyberdéfense. Mais au-delà de son rôle de conseil, elle n'est pas en mesure d'agir sur le terrain en soutien direct lors de potentielles attaques.

Car dans le cadre d'une Union Européenne dépourvue de forces armées communes, la défense cyber relève encore entièrement de la souveraineté nationale des États. Chaque pays se munit donc de sa propre agence et de sa propre politique. La France par exemple dispose de l'agence nationale de la sécurité des systèmes d'informations (ANSSI).

C'est une faiblesse car l'unité du monde cyber implique des attaques à grande échelle, touchant des zones qui peuvent s'étendre à plusieurs continents. Une Union qui ne peut se protéger des ingérences extérieures lors d'élections ou qui peut se faire submerger par un ver informatique[1] à tout moment est sensible à des attaques qui peuvent détruire son économie ou paralyser ses armées à certains moments critiques.

Où en est-on aujourd'hui ? Quelle est la position européenne sur la coopération en matière de cyber, et que peut-on en espérer pour le futur ?

Une Europe de la défense à plusieurs vitesses

L'Union Européenne n'ayant pas de cyberdéfense propre, seulement des organismes de coopérations, chaque État est responsable de sa propre protection. Dès lors, il y a une très grande diversité de protection entre les pays. On peut distinguer trois cas. L'Europe de l'Ouest,

[1] Un ver informatique est un logiciel malveillant qui infecte différents ordinateurs via internet. Il est complètement autonome (contrairement aux virus) et peut se reproduire de lui-même sans aide d'un quelconque logiciel.

à un stade plutôt avancé et qui a pris conscience de l'ampleur du danger. L'Europe centrale, se reposant sur une protection dans le cadre de l'OTAN. Et le cas, très particulier, de l'Estonie.

L'Europe de l'Ouest tout d'abord. Certains pays comme la France ou l'Allemagne ont bien pris conscience de l'importance du phénomène. La France est déjà reconnue pour sa politique de cyberdéfense, l'ANSSI et le commandement de la cyberdéfense française ont gagné l'exercice LockedShields en 2019 qui consiste en une compétition entre alliés de l'OTAN afin de voir qui parviendra le mieux à protéger un pays fictif d'une cyberattaque. Elle a également récemment été classée 2ème puissance en cyberdéfense par un rapport du Belfer Center, un centre de recherche associé à Harvard.[2] Enfin, la France est par ailleurs un des rares pays à posséder une doctrine de lutte offensive, celle-ci a en effet été en 2019 dévoilée par Mme Florence PARLY.[3] De même, l'Allemagne s'est vite dotée d'une unité de cyberdéfense en 2017 formant une nouvelle branche de l'armée pour contrer spécifiquement les attaques russes après un piratage de grande ampleur du Bundestag en 2015. Elle a annoncé l'année dernière développer l'aspect offensif de ses forces cyber et ne plus se consacrer qu'au défensif. D'autre part, elle devrait mettre à disposition l'ensemble de ses forces au service de l'OTAN. On peut également citer les forces néerlandaises et espagnoles qui font un important travail de construction d'une force cyber[4].

Cependant, certains pays en Europe centrale ont une approche différente. Pour certaines nations la cyber sécurité est l'affaire d'autorités civiles (d'où l'idée de cyber sécurité et non de cyber défense). Les cyberattaques sont criminalisées et traitées de manière interne et sans lien avec l'armée. Ainsi, en République Tchèque, la cyberdéfense est du ressort de l'agence nationale de sécurité et du ministre de l'intérieur, le ministre de la défense ne s'occupant que des questions en liens avec l'OTAN. La Slovaquie place la cyberdéfense dans le giron du ministre des finances. En Hongrie, la cyberdéfense se base principalement sur la coopération internationale (notamment de l'OTAN) et se compose d'autorités nationales modestes. Les questions de cyberdéfense sont analysées sous le spectre du danger économique et sécuritaire plus que sur la question de la protection de la souveraineté de l'État. Les actions se focalisent sur une responsabilisation des individus et des entreprises plutôt que sur l'aspect de défense

[2] https://www.challenges.fr/entreprise/defense/la-france-6eme-puissance-cyber-mondiale_728980.
[3] https://www.defense.gouv.fr/actualites/articles/cyberdefense-la-france-passe-a-l-offensive.
[4] https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf.

nationale. Il est important de préciser que certains pays comme les pays baltes (dont l'Estonie citée précédemment) et la Pologne organisent quand même une défense plus soutenue.[5] Mais la région reste peu encline à répondre aux immiscions dans leur espace cyber. Parmi la centaine d'attaques ayant été recensées dans cette région en 2017, moins d'un quart a été pris en charge par les autorités étatiques[6].

Enfin, il y a le cas très particulier de l'Estonie. Ce pays est en effet à la fois le premier pays à avoir subi une cyberattaque visant directement un Etat, et l'un des plus avancé dans la cyberdéfense. Fin Avril 2007, l'Estonie a fait face à une cyberattaque massive en « déni de service ». Ce type d'attaque consiste à saturer des serveurs de requêtes jusqu'à ce qu'ils ne puissent plus fonctionner. Les serveurs – en l'occurrence une partie importante des services publics et des grands organismes estoniens – se sont retrouvés alors hors de service et le pays fut à l'arrêt. La puissance informatique nécessaire pour une attaque de cette ampleur nécessite l'implication d'un État. Ici, l'Estonie n'a pas tardé à dénoncer la Russie, même s'il lui était impossible (et encore aujourd'hui) d'en apporter la preuve.

Cette cyberattaque a été le catalyseur d'une révolution. L'Estonie a développé une société presque entièrement connectée : les estoniens bénéficient d'une carte d'identité électronique qui remplace toutes les autres pièces officielles. Avec un compte commun pour la grande majorité de l'administration, ils peuvent accéder à 99 % de leurs services publics en ligne et près de la moitié des citoyens ont voté en ligne lors des dernières élections.[7] Notons par ailleurs que l'administration n'a pas le droit de demander deux fois la même information à un citoyen au long de sa vie. Pourtant cette société connectée est aussi des plus sécurisées, l'année suivant l'attaque, l'OTAN s'installe à Tallinn en créant le centre d'excellence de cyberdéfense coopérative. Centre militaire au cœur de la coopération occidentale de cyberdéfense. Se préparant chaque année à travers l'exercice « LockedShields ». L'Estonie est aujourd'hui en avance sur la digitalisation de la société mais également dans sa sécurisation.

Ces disparités en Europe entrainent des problèmes de fond lors de la mise en place de politiques communes. Certains pays comme le Royaume-Uni ou la France ont fait barrage à

[5] https://www.researchgate.net/publication/312508248_CYBERSECURITY_IN_CENTRAL_EASTERN_EUROPE_FROM_IDENTIFYING_RISKS_TO_COUNTERING_THREATS.
[6] https://cms.law/en/hun/publication/the-cybersecurity-challenge-in-central-and-eastern-europe.
[7] https://www.eyes-on-europe.eu/estonie-la-societe-digitale-par-excellence/.

certaines dispositions lors de négociations de traités pour une politique cyber de l'UE par peur de partager des informations trop avancées et trop sensibles à leurs alliés. Il y a en général une peur de nivellement par le bas de la cyber défense en Europe[8].

Certains pays peu avancés ne coopèrent que très peu et souhaitent d'abord développer leur cyber défense souveraine. La logique est que beaucoup de pays de l'UE sont déjà sous la protection importante de l'OTAN en matière de cyberdéfense, ce qui rend inutile une autre force cyber de coopération alors même que ces pays n'ont pas d'armée viable dans ce domaine.

L'OTAN est restée pendant longtemps l'acteur majeur de la cyber sécurité des pays de l'Union Européenne. Jens STOLTENBERD, le secrétaire général de l'organisation a déclaré que l'article 5 du traité (sur la défense collective) pouvait être invoqué en cas d'attaque cyber contre un membre qui deviendrait une attaque contre tous les alliés, garantissant une protection de poids pour les pays européens[9]. D'autant qu'en plus de la force américaine, certains pays mettent leurs capacités cyber à la disposition des opérations et des missions de l'OTAN. Il ne s'agit pas ici de se délester de la souveraineté de la gestion d'une branche de leur armée, mais de permettre à l'organisation d'utiliser les forces des pays si besoin pour le bien des alliés. Le Royaume-Uni, le Danemark, les Pays-Bas, l'Estonie ainsi que l'Allemagne sont dans ce cas[10]. Ce sont les pays européens avec les technologies les plus développées en matière de cyber qui rejoignent les États-Unis dans ce partage des forces développant une puissance défensive certaine. En plus de cette force importante, l'OTAN a fait preuve d'une grande réactivité, dès 2007 et à la suite de l'attaque contre l'Estonie, les ministres de la Défense des alliés ont établi la nécessité d'un « travail urgent » dans le domaine. Des 2008 la première politique commune de cyberdéfense, le centre d'excellence de cyberdéfense et la rédaction du Manuel Talinn (finalisé en 2013) sont mis en place. Ce manuel se veut comme une transposition du droit international au monde cyber, plaçant ce type d'attaque au même plan qu'une attaque physique contre un État.

[8] https://www.taurillon.org/l-emergence-d-une-politique-europeenne-de-cybersecurite?lang=fr.
[9] https://www.nato.int/cps/fr/natohq/news_168435.htm?selectedLocale=fr.
[10] http://www.opex360.com/2019/02/14/lallemagne-va-mettre-ses-capacites-en-matiere-de-cyberdefense-a-la-disposition-de-lotan/.

L'OTAN est aujourd'hui encore la garantie de sécurité de l'Union Européenne contre les attaques extérieures étatiques. L'organisation est aussi une pionnière dans la discipline, dispose de moyens conséquents et un rôle influent.

Cette omniprésence de l'OTAN sur les questions de cyber sécurité a conduit l'Union Européenne à négliger toute tentative d'autonomie stratégique dans ce domaine. On observe cependant une prise de conscience progressive de l'Union de l'importance d'établir sa propre cyberdéfense.

Une prise de conscience tardive mais efficace

A la suite de la crise de 2007 en Estonie, l'ENISA n'avait pas les compétences d'agir sur le terrain, en soutien direct. De manière générale, à la suite de cette attaque l'Union Européenne n'a pas réellement eu d'action tangible pour protéger ses membres, et se repose sur l'action active et efficace de l'OTAN en la matière.

Un embryon de politique de cyberdéfense commune apparait tout de même en 2016 avec l'adoption de la directive SRI (Sécurité des réseaux et des systèmes d'information). C'est le premier cadre législatif s'accordant sur tout l'UE[11]. Ce cadre, transposé en 2018 met en place une obligation d'audit pour les entreprises, des notifications d'incidents et élabore des mesures de sécurité pour les entreprises. L'objectif étant moins la cyberdéfense de l'union qu'une première protection de l'ensemble du territoire face aux virus malveillants envoyés de l'étranger pouvant soutirer information ou argent d'entreprises de l'UE. Cette directive est le point de départ d'une collaboration renforcée entre les pays, et votée à l'unanimité, elle montre un début de prise de conscience. Mais cette prise de conscience ne signifie pas pour autant un accord total. Les dissensions - exposées plus haut - entre les différents pays empêchaient la mise en place d'une politique efficace, contraignante, avec un effet certain sur la défense européenne.

Moins d'un an après l'adoption – mais avant la transposition – de cette directive, deux vers informatiques touchent le monde entier : Wannacry et Notpetya. Ces vers sont des exemple types de ce que la directive SRI est censée permettre d'éviter. En mai et juin 2017, ils ont affecté

[11] https://ec.europa.eu/commission/presscorner/detail/fr/MEMO_18_3651.

des centaines de milliers d'ordinateurs du monde entier. Se présentant comme des *ransomware*, ils bloquent l'accès des ordinateurs et proposent de rendre cet accès en échange d'une rançon. Ces attaques ont fait plusieurs milliards de dollars de dégâts et sont considérés comme les plus grandes cyberattaques de l'histoire[12]. Elles sont d'autant plus dangereuses qu'aujourd'hui encore la communauté internationale n'a pas trouvé de responsable pour aucune des attaques. De plus, en 2016 et 2017 avec les soupçons d'ingérence russe dans les élections américaines et françaises, la communauté internationale prend conscience de l'urgence d'agir de manière plus efficace et coordonnée contre les intrusions extérieures dans le cyber espace d'un pays.

En réaction à ces deux phénomènes, à partir de 2017, l'Union Européenne a commencé à agir de manière coordonnée et à une échelle ambitieuse. C'était l'objectif du sommet européen de Talinn le 19 septembre 2017. Il proposait d'une part, de créer une nouvelle politique, plus ambitieuse que la directive SRI pour se protéger des vers tels que Wannacry. D'autre part, il créait une nouvelle agence, en continuité de l'ENISA pour assister les États directement contre les cyberattaques. De plus, une recommandation de la commission européenne fut prise pour permettre à Europol d'agir en partenariat avec l'ensemble des pays pour aider les victimes de cyberattaques à se défendre et limiter les dégâts. Elle mettait en place des réseaux de communication sécurisés, des points permanents d'échange d'information entre les pays[13].

Une nouvelle dynamique, la prise de conscience au niveau européen, voit donc le jour en 2017 et s'est développée depuis.

Premièrement, à travers la Coopération Structurée Permanente (PESCO). Cette coopération structurée est prévue par le traité de Lisbonne pour approfondir la coopération dans le domaine de la sécurité et de la défense des États-membres. C'est donc bien une approche militaire qui est prise.

Parmi les toutes premières propositions de coopération, la Lituanie a avancé la mise en place d'une cyber force commune pour répondre aux crises transfrontalières : la *cyber rapid response teams and mutual assistance in cyber security*. Cette assistance regroupe des unités spécialisées de chaque pays participant. Ces unités sont mobilisables en commun pour renforcer la défense

[12] https://fr.wikipedia.org/wiki/WannaCry#cite_note-:3-6.

[13] https://cyberguerre.numerama.com/1118-avec-son-nouveau-protocole-de-cyberdefense-lue-veut-se-proteger-des-cyberattaques-majeures-a-venir.html.

d'un pays particulier en cas d'attaque. Elle regroupe aujourd'hui la Lituanie, l'Estonie, la Croatie, la Roumanie, l'Espagne et les Pays-Bas et il s'agit d'un des projets les plus avancés dans le cadre de PESCO.

A la suite du succès de ce projet, 8 autres propositions ont été mises en place[14]. Elles ont été lancées par différents pays et regroupent chacune une partie des membres. On peut notamment citer l'initiative française pour le développement de technologies radios militaires communes et sécurisées (ESSOR), l'initiative grecque pour le développement de mesures de défenses communes (pour l'instant il s'agit principalement de pare-feu communs), ou encore le projet commun à l'Espagne et au Portugal pour le développement d'une école du cyber et de l'innovation pour former des experts dans le domaine (EU CAIH).

Enfin, toujours dans une logique de coopération, l'ENISA met en place depuis 2019 l'évènement Blue Olex pour renforcer l'échange de connaissance dans l'UE[15]. Organisé en France en 2019 puis aux Pays-Bas cette année, cet évènement veut à terme préparer une discussion politique sur la cyberdéfense en rassemblant des hauts responsables des 27. A cet effet, l'évènement de cette année a permis la mise en place de CYCLONE avec l'idée d'établir un niveau intermédiaire entre politique et technique dans la gestion des crises cyber.[16] L'objectif est de permettre une analyse globale et efficace en réponse aux crises cyber entre les pays.

Cette multiplication d'initiatives montre l'intérêt de l'Europe à coopérer dans ce domaine pour conserver sa souveraineté face aux attaques extérieures.

Vers une souveraineté européenne en matière de cyber ?

A terme, il est possible d'entrevoir une UE autonome en cyberdéfense. Mais il existe de nombreux obstacles à une telle autonomie.

Un premier obstacle à cette autonomie réside dans la réticence des pays à partager des informations et des prérogatives de souveraineté, particulièrement concernant la défense. Sans refaire l'histoire de la CED et des différentes initiatives de défense européenne échouées, l'Union Européenne est réticente à mutualiser sa défense y compris dans le domaine cyber.

[14] https://www.consilium.europa.eu/media/41333/pesco-projects-12-nov-2019.pdf.
[15] https://www.enisa.europa.eu/news/enisa-news/blue-olex-2020-the-european-union-member-states-launch-the-cyber-crisis-liaison-organisation-network-cyclone.

Certains pays plus avancés ne veulent pas partager des informations trop sensibles de peur qu'elles soient ensuite transférées dans des pays moins sécurisés et finalement volés lors d'une attaque sur ce pays membre de l'UE mais avec des standards de sécurités moindres.

Un deuxième obstacle concerne la coopération déjà forte avec l'OTAN. Certains pays de l'UE avec une cyberdéfense sous-développée souhaitent d'abord développer leur défense nationale, considérant que la protection actuelle de l'OTAN est suffisante. Même les pays les plus avancés se fondent aujourd'hui sur l'organisation, on l'a vu avec l'Allemagne qui va rejoindre les Pays-Bas dans la mise à disposition de ses forces au service de l'OTAN et non au service de l'Union Européenne. La puissance cyber de l'OTAN et sa prise de conscience rapide ayant permis un travail de fond depuis plus d'une décennie en font une force considérable. Pour beaucoup, il n'y a pas beaucoup d'intérêt de sortir de cette protection pour en créer une autre autonome, mais moins forte.

Ces quelques obstacles ne doivent toutefois pas faire oublier les avancées conséquentes de l'Union Européenne dans la coopération. Dans ce domaine, il est important d'avoir des pays moteurs qui lancent des dynamiques de plus en plus ambitieuses dans la coopération cyber de l'Union. On peut citer la Pologne qui reste certes sous le parapluie de l'OTAN mais renforce ses forces nationales et coopère dans beaucoup de domaines avec l'UE et la France. Cette dernière n'a pas mis à contribution ses forces avec l'OTAN, préférant lancer beaucoup de projets européens de défense, c'est ce que précisait Emmanuel Macron dans son appel de Paris de 2018, appelant à une puissance européenne cyber autonome. Ces deux pays moteurs sont rejoints par les pays baltes, avec l'Estonie qui est pionnière en la matière et la Lituanie qui souhaite développer ses capacités en coopération totale avec l'Union Européenne.

Finalement, l'Union Européenne est traversée de nombreux dilemmes et désaccords de fond sur sa gestion commune de la cyberdéfense. Entre les pays considérant que le cyber relève du civil, ceux qui se fondent sur le parapluie de l'OTAN et ceux qui ont peur de partager des informations à des pays trop peu avancés en matière de sécurité, l'UE a de nombreux défis à relever avant d'arriver à une défense autonome et efficace contre les géants des attaques cyber comme la Chine ou les États-Unis. Cependant, les avancées sont présentes, elles sont multiples et parfois confuses mais dans une direction certaine de renforcement de la puissance cyber européenne.

publication@jeunes-ihedn.org