Hughes Hubbard & Reed

Adoption des toutes premières sanctions économiques européennes en matière de cybermalveillance

Client Advisories

Hughes Hubbard & Reed LLP • A New York Limited Liability Partnership
One Battery Park Plaza • New York, New York 10004-1482 • +1 (212) 837-6000

Attorney advertising. Readers are advised that prior results do not guarantee a similar outcome. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. For information regarding the selection process of awards, please visit https://www.hugheshubbard.com/legal-notices-methodologies.

8 septembre 2020 - Confrontée à la multiplication des cyberattaques qui tendent à mettre à mal l'intégrité, la sécurité et la compétitivité des acteurs économiques européens, l'Union européenne a renforcé ces dernières années sa capacité à dissuader et répondre aux cyber-menaces et aux cyber-activités malveillantes. Ainsi, l'Union européenne (« UE ») s'est, le 30 juillet 2020, appuyée pour la première fois sur l'arsenal règlementaire mis en place ces dernières années pour imposer des sanctions économiques à l'encontre de six (6) personnes civiles et trois (3) personnes morales au titre de leur participation (i) aux cyberattaques contre l'Organisation pour l'interdiction des armes chimiques, (ii) aux attaques « WannaCry », « NotPetya » et (iii) à l'opération « Cloud Hopper ».

Présentation de l'arsenal règlementaire européen

Les premières désignations de l'UE survenues le 30 juillet 2020 sont l'aboutissement d'un long processus débuté le 19 juin 2017, par l'adoption par le Conseil de l'UE de conclusions relatives à la mise en place d'un cadre pour une réponse diplomatique conjointe aux cyber-activités malveillantes prenant la forme d'une « boîte à outils de cyber-diplomatie ». Cette « boite à outils » permet à l'UE de s'appuyer sur les outils existants de politique extérieure et de sécurité commune (« PESC ») pour protéger l'intégrité et la sécurité de l'UE et de ses Etats membres.[1]Parmi les outils existants pouvant être utilisés dans ce nouveau cadre, le Conseil de l'UE évoque les « mesures restrictives » ou sanctions économiques.

C'est à ce titre que le 17 mai 2019, le Conseil de l'UE a, au travers d'une décision PESC et d'un règlement correspondant, mis en place un cadre pour imposer des mesures restrictives ciblées à l'encontre de personnes ou entités (et toute personne associée) responsables de cyberattaques ou de tentatives de cyberattaques, qui apportent un soutien financier, technique ou matériel à ces cyberattaques, ou sont impliquées de toute autre manière dans celles-ci [2]. Ces mesures restrictives comprennent notamment à l'encontre des personnes

sanctionnées des interdictions de voyager vers et au sein de l'UE ainsi que des mesures de gel des avoirs comprenant l'interdiction de mise à disposition de fonds ou ressources économiques.

Première utilisation de cet arsenal règlementaire : présentation de la décision du Conseil et du règlement d'exécution correspondant

Ce cadre règlementaire a été utilisé pour la première fois, par une décision du Conseil et un règlement d'application correspondant le 30 juillet 2020, imposant des sanctions économiques à six (6) personnes civiles et trois (3) personnes morales pour leur participation (i) aux cyberattaques contre l'Organisation pour l'interdiction des armes chimiques, (ii) aux attaques « WannaCry », « NotPetya » et (iii) à l'opération « Cloud Hopper ».[3]

Les mesures restrictives mises en place visent ainsi :

- 2 personnes physiques chinoises (*Gao Qiang* et *Zhang Shilong*) pour leur participation à l'opération « Cloud Hopper » qui ciblait les systèmes d'information de sociétés multinationales sur six continents, y compris des entreprises situées dans l'Union européenne en récupérant des informations commercialement sensibles, entraînant des pertes économiques importantes et un organisme chinois (*Tianjin Huaying Haitai Science and Technology Development Co.*) pour avoir fourni un soutien financier, technique ou matériel et facilité « l'opération Cloud Hopper » ;
- 4 personnes physiques russes (*Alexey Valeryevich Minin, Aleksei Sergeyvich Morenets, Evgenii Mikhaylovich Serebriakov, Oleg Mikhaylovich Sotnikov)* pour leur participation à une tentative d'attaque contre l'Organisation pour l'interdiction des armes chimiques aux Pays-Bas et un organisme étatique russe (*Centre principal pour les technologies spéciales (GTsST) de la Direction principale de l'état-major général des forces armées de la Fédération de Russie (GU / GRU)*) pour sa participation aux attaques « NotPetya » ou « EternalPetya » qui ont paralysé les données de plusieurs grandes entreprises (comme Merck ou Auchan) en ciblant les ordinateurs avec des *ransomwares* et en bloquant l'accès aux données, entraînant entre autres des pertes économiques importantes ainsi qu'une cyberattaque contre un réseau électrique ukrainien provoquant sa paralysie partielle pendant l'hiver ;
- une société nord-coréenne (*Chosun Expo*) pour avoir fourni un soutien financier, technique ou matériel et facilité une série de cyberattaques ayant un effet significatif, provenant de l'extérieur de l'Union européenne et constituant une menace externe pour l'UE ou ses Etats membres et des cyberattaques contre des Etats tiers, y compris les cyberattaques publiquement connues sous le nom de « WannaCry » ayant perturbé les systèmes d'information d'entreprises de l'UE et du monde entier en ciblant les systèmes d'information avec des *ransomwares* et en bloquant l'accès aux données.

Les sanctions imposées comprennent une interdiction de pénétrer sur le territoire de l'UE et de circuler en son sein ainsi qu'un gel des avoirs au titre duquel il est interdit aux personnes et aux entités de l'UE de mettre des fonds à la disposition des personnes et entités inscrites sur la liste.

Si les mesures restrictives européennes sont d'applicabilité directe (dans la mesure où elles sont prononcées au travers d'un règlement européen), les Etats membres demeurent libres de déterminer les infractions prévues en présence d'une contravention aux dispositions dudit règlement (article 15 du Règlement (UE) 2019/796 du Conseil du 17 mai 2019).[4] A titre d'exemple, en France, le Code des douanes et le Code pénal prévoient des sanctions pénales pour la violation des mesures restrictives européennes. Ces sanctions sont prévues au 1 bis et 1 ter de l'article 459 du Code des douanes.

Une réaction américaine plus rapide et virulente

Egalement confrontés à ces cyber-menaces, les Etats-Unis se sont emparés très tôt du sujet en adoptant dès 2015 l'*Executive Order 13694 [5]* instaurant un cadre règlementaire au titre duquel les personnes responsables ou

complices de cyberattaques menées depuis l'étranger contre des intérêts américains et représentant une menace à la sécurité nationale, à la politique étrangère, à l'économie et à la stabilité financière des Etats-Unis peuvent être désignés sur la liste de gel des avoirs américaine (*OFAC's List of Specially Designated Nationals and Blocked Persons - SDN List*). Ces sanctions imposent un gel des avoirs détenus par ces personnes sur le territoire américain et interdisent à toute *U.S. person* d'entrer ou d'entretenir une relation d'affaires avec un SDN.

A la suite de l'interférence russe dans l'élection présidentielle américaine, cet *Excutive Order* a été amendé par l'*Executive Order 13757 du* 28 décembre 2016 sur le fondement duquel des sanctions à l'encontre de cybercriminels russes considérés comme responsables de ces interférences ont été prononcées.

D'autres sanctions analogues ont été prononcées ces dernières années sur le fondement de l'*Executive Order 13694* :

- en septembre 2017 à l'encontre d'une (1) société iranienne et trois (3) personnes physiques pour avoir causé des perturbations au sein des systèmes d'information de plusieurs banques américaines en 2011 et 2012 et quatre (4) autres personnes physiques pour avoir perturbé les systèmes d'information de plusieurs sociétés en travaillant pour le compte de Mersad, une société de sécurité iranienne affiliée aux gardiens de la révolution islamique ;[6]
- en mars 2018 à l'encontre de trois (3) organismes et treize (13) personnes physiques russes pour avoir participé à des activités cybercriminelles en ce compris l'interférence dans l'élection présidentielle américaine ; [7]
- en mars 2018 à l'encontre d'un (1) organisme et dix (10) personnes physiques iraniennes pour avoir volé des données en ligne appartenant à des universités américaines et divers médias ;[8]
- en février 2019 à l'encontre d'une (1) société iranienne et (6) personnes physiques impliquées dans des cyberattaques contre des membres du gouvernement américain et des forces armées ;[9]
- en décembre 2019 à l'encontre de sept (7) organismes et dix-sept (17) personnes physiques russes impliquées dans la conception et la propagation du virus « Dridex » ;[10]
- en juin 2020 à l'encontre de six (6) cybercriminels nigérians pour avoir mis en place en ligne un schéma frauduleux permettant d'extorquer plus de six millions de dollars à des citoyens américains[11]

D'autres sanctions ont également été prononcées sur le fondement de l'*Executive Order 13772* relatif au programme de sanctions nord-coréen ;

- en septembre 2018 à l'encontre d'un (1) programmeur nord-coréen et une (1) société nord-coréenne (*Chosun Expo*) pour avoir notamment participé dans l'attaque « WannaCry » et l'attaque contre Sony en novembre 2014 ;
- en septembre 2019 à l'encontre de trois (3) organismes nord-coréens (*Lazarus Group, Bluenoroff, Andariel)* bénéficiant de l'appui des services de renseignement nord-coréens pour avoir cibler des infrastructures américaines.[12]

Il est ici intéressant de noter que les auteurs de ces attaques ont été désignés par les autorités américaines deux ans avant leur désignation par l'Union européenne en juillet 2020 au titre des premières sanctions européennes prononcées pour des actes de cyber-malveillance, ce qui symbolise le plus fort activisme des autorités de poursuites américaines.

Evolutions et perspectives

Bien qu'inédites et bienvenues, ces mesures de sanctions économiques européennes arrivent tardivement et la question de leur efficacité et de leur proportionnalité doit dans ce contexte être posée. C'est la première fois que l'Union européenne répond fermement à ces actes de cybermalveillance et semble ainsi prendre la mesure du

risque auquel nombre d'entreprises européennes font face presque quotidiennement. Pour autant, cette décision est-elle à la hauteur de ce danger protéiforme et en perpétuelle évolution ? L'Union européenne n'a-t-elle pas tardé à agir ? Ces sanctions seront-elles dissuasives pour des pirates informaticiens dont la présence est indétectable et les avoirs financiers difficilement traçables ?

Ces sanctions s'inscrivent en tout état de cause dans une utilisation exponentielle de cet outil juridique longtemps décrié mais dont le retour en grâce s'est opéré à l'été 2014 lors de l'imposition de sanctions économiques sectorielles contre les intérêts économiques russes à la suite de l'annexion du territoire de Crimée et de la participation des forces russes dans l'insurrection du Donbass. Les 5 dernières années ont vu, tant du côté européen que du côté américain, l'imposition ou le renforcement de régimes de sanctions économiques contre l'Iran, le Venezuela, la Turquie (brièvement) et maintenant la Chine comme alternatives à des interventions armées contre ces mêmes territoires. Parallèlement, l'activisme des régulateurs américains, et notamment de l'*Office of Foreign Assets Control*, a renforcé la portée contraignante de ces mesures sur les entreprises occidentales actives dans ces pays.

La situation politique en Biélorussie, les tensions relatives à l'imposition de sanctions onusiennes envers l'Iran (embargo sur les armes), l'ingérence de Pékin à Hong Kong, les accusations d'espionnage de l'administration américaine à l'encontre de réseaux sociaux chinois sont autant de sujets qui préfigurent des évolutions notables en matière de sanctions économiques. Les prochains mois (et c'est dans ce contexte que d'autres brèves sanctions économiques seront publiées chaque semaine) devraient donc être riches en développements et enseignements.

_____

[1] Communiqué de presse du Conseil de l'UE, « Cyberattaques : l'UE est prête à réagir par une série de mesures, y compris des sanctions ».

[2] Décision du (PESC) 2019/797 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses Etats membreset Règlement (UE) 2019/796 du Conseil du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses Etats membres.

[3]Décision (PESC) 2020/1127 du Conseil du 30 juillet 2020 modifiant la décision (PESC) 2019/797 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses Etats membres et Règlement d'exécution (UE) 2020/1125 du Conseil du 30 juillet 2020 mettant en œuvre le règlement (UE) 2019/796 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses Etats membres.

[4] Règlement (UE) 2019/796 du Conseil du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses Etats membres.

[5]https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.

[6]https://home.treasury.gov/news/press-releases/sm0158.

[7]https://home.treasury.gov/news/press-releases/sm0312.

[8] https://home.treasury.gov/news/press-releases/sm0332.

[9]https://home.treasury.gov/news/press-releases/sm611.

[10]https://home.treasury.gov/news/press-releases/sm845.

[11]https://www.state.gov/u-s-sanctions-nigerian-cyber-actors-for-targeting-u-s-businesses-and-individuals/.

[12]https://home.treasury.gov/news/press-releases/sm774.

Related People

Olivier Dorgans

Paul Charlot

Camille Mayet

Nicolas Burnichon

Related Areas of Focus

Sanctions, Export Controls & Anti-Money Laundering
Data Privacy & Cybersecurity

In English