Het EU-cybersanctieregime van 2019 als antwoord op cyberdreigingen en kwaadwillige cyberactiviteiten

written by Dennis_ Rombaut_ | november 5, 2021

Het EU-cybersanctieregime van 2019 als antwoord op cyberdreigingen en kwaadwillige cyberactiviteiten

Op 17 mei 2019 heeft de Raad van de Europese Unie (hierna: Raad) een juridisch kader gecreëerd om door middel van gerichte beperkende maatregelen te reageren op de stijgende trend van georganiseerde cyberaanvallen met aanzienlijke gevolgen die een externe bedreiging vormen voor de Unie of haar lidstaten.[1]

Zo kan de Raad voortaan een verbod opleggen om enerzijds naar de EU te reizen[2] of kan ze anderzijds alle geldmiddelen bevriezen die toebehoren aan natuurlijke personen of rechtspersonen die op enige wijze betrokken zijn bij cyberaanvallen of pogingen tot cyberaanvallen.[3] Dergelijke maatregelen moeten dienen als afschrikking.

Bovendien moeten zij onderscheiden worden van het aansprakelijk stellen van een derde Staat voor cyberaanvallen. De toepassing van gerichte beperkende maatregelen komt niet neer op een aansprakelijkheidstelling, wat steeds een soeverein politiek besluit blijft dat op een individuele basis wordt genomen. Het staat iedere lidstaat wel vrij om de aansprakelijkheidsstelling van een derde Staat met betrekking tot cyberaanvallen zelf te bepalen.[4] De Uniewetgever wil op die manier de juridische, technische en politieke moeilijkheden vermijden die rijzen bij het toerekenen van een cyberaanval aan een Staat.[5]

Onder cyberaanvallen verstaat de verordening van 17 mei 2019 één van de volgende activiteiten:

- zich toegang verschaffen tot informatiesystemen;
- verstoren van informatiesystemen;
- verstoren van gegevens;
- onderscheppen van gegevens.

Cyberaanvallen die een externe bedreiging vormen, omvatten onder meer degene

die ofwel afkomstig zijn, of worden uitgevoerd, van buiten de Unie, ofwel gebruik maken van infrastructuur buiten de Unie, dan wel worden uitgevoerd door natuurlijke of rechtspersonen die buiten de Unie zijn gevestigd of actief zijn, of worden uitgevoerd met de steun van natuurlijke personen of rechtspersonen die buiten de Unie actief zijn.

Een cyberaanval kan dan ook een bedreiging vormen voor een lidstaat indien informatiesystemen worden aangevallen die bijvoorbeeld betrekking hebben op de kritieke infrastructuur, of diensten die nodig zijn voor het in stand houden van essentiële sociale en/of economische activiteiten, of kritieke functies van de staat zoals op het gebied van defensie en van het bestuur en het functioneren van de instellingen.[6]

Met de SolarWinds-cyberaanval op de Amerikaanse federale regering, de cyberaanval op het Duitse federale parlement in 2015 en de recente cyberaanval op het Europees Geneesmiddelenbureau van Pfizer en BioNTech is het duidelijk dat cyberbeveiliging steeds relevanter wordt.[7] Al op 19 juni 2017 nam de Raad conclusies aan over een kader voor een gezamenlijke diplomatieke reactie op kwaadwillige cyberactiviteiten. Het zogenaamde Instrumentarium voor cyberdiplomatie waarin de Raad zijn bezorgdheid uitte over de toegenomen capaciteit en bereidheid van Staten en niet-statelijke actoren om via kwaadwillige cyberaanvallen hun doelstellingen te bereiken. De Raad wees toen al op de groeiende behoefte aan bescherming van de integriteit en veiligheid van de Unie, haar lidstaten en haar burgers tegen cyberbedreigingen.[8]

Besluit

Zoals hierboven werd beschreven, kiest de Uniewetgever met het cybersanctieregime voor het sanctioneren van niet-statelijke actoren om op die manier politieke en diplomatieke moeilijkheden te vermijden. Het cybersanctieregime sluit het toeschrijven van de verantwoordelijkheid voor een cyberaanval aan een Staat expliciet uit. Het toerekenen van een cyberaanval aan een Staat kan immers aanzienlijke politieke spanningen teweegbrengen. Het is maar de vraag of de Uniewetgever op die manier geen juridische fictie creëert. De meerderheid van voorkomende cyberaanvallen wordt immers op verzoek van of met de steun van overheden uitgevoerd, zoals Stuxnet[9], Wannacry[10] en NotPetya[11]. Bovendien zal de schijn van toerekening aan een Staat blijven bestaan wanneer de Unie cybersancties uitvaardigt tegen een onderdaan van die bepaalde derde Staat.[12]

Indien u na het lezen van dit artikel nog vragen hebt, aarzel dan niet om ons te contacteren via joost.peeters@studio-legale.be of 03 216 70 70.

[1] Zie overweging (7) van het BESLUIT (GBVB) 2019/797 VAN DE RAAD van 17 mei 2019 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen; VERORDENING (EU) 2019/796 VAN DE RAAD van 17 mei 2019 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen.

[2] Zie artikel 4 van het BESLUIT (GBVB) 2019/797 VAN DE RAAD van 17 mei 2019 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen.

[3] Zie artikel 5 van het BESLUIT (GBVB) 2019/797 VAN DE RAAD van 17 mei 2019 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen. Zie artikel 3 van de VERORDENING (EU) 2019/796 VAN DE RAAD van 17 mei 2019 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen.

[4] Zie overweging (8) en (9) van het BESLUIT (GBVB) 2019/797 VAN DE RAAD van 17 mei 2019 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen.

[5] A.VERHELST, M.RUELENS en J. WOUTERS., "Het EU-cybersanctieregime en zijn verenigbaarheid met de grondrechten in het Unierecht", *RW* 2021-22, nr. 02, 11 september 2021, p.52.

[6] https://ecer.minbuza.nl/-/een-eu-cybersanctieregime-stap-voor-meer-veiligheid-in-cyberspace

[7] A.VERHELST, M.RUELENS en J. WOUTERS., "Het EU-cybersanctieregime en zijn verenigbaarheid met de grondrechten in het Unierecht", *RW* 2021-22, nr. 02, 11 september 2021, p.43.

[8] Zie overweging (1) van het BESLUIT (GBVB) 2019/797 VAN DE RAAD van 17 mei 2019 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen.

[9] De Stuxnet-cyberaanvallen tegen Iraanse nucleaire faciliteiten waren volgens sommige bronnen een gezamenlijke operatie van de Verenigde Staten en Israël. Zie DUMORTIER, V.PAPAKONSTANTINOU en P. DE HERT, "EU sanctions against cyber-attacks and defense rights: Wanna-Cry?", *European Law Blog* 2020, 2 en J. KAMBIC en S. LILES, "Non-State Cyber Power in ONG", *Journal of Information Warfare* 2014, 57-67.

[10] WannaCry was een uitbraak van ransomware die zich richtte op het Windowsbesturingssyteem in verscheidende landen. Zie VK, Departement van Buitenlandse Zaken, "Foreign Office Minister condems North Korean actor for WannaCry attacks", Persmededeling 19 december 2019, online beschikbaar op https://gov.uk/government/news/foreign-office-minister-condems-north-korean-actor-for-wannacry-attacks en G. FUSTER L. JASMONTAITE, "Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights" in M.CHRISTEN, B.GORDIJN en M.LOI (eds.), *The Ethics of cybersecurity*, Cham, Springer, 2020, 99-100.

[11] De NotPetya-aanval was een uitbraak van ransomware die opnieuw het Windowsbesturingssysteem viseerde. Zie VK, Departement van Buitenlandse Zaken en Nationaal Centrum voor Cyberbeveiliging, "Foreign Office Ministers condems Russia for NotPetya attacks", Nieuwsmededeling 15 februari 2018; B. BLUMBERGS, K. VAN DER MEIJ en L.LINDSTRÖM, "NotPetya and WannaCry Call for a Joint Response from International Community", NATO Cooperative Cyber Defence Centre of Excellence Paper 2018.

[12] A.VERHELST, M.RUELENS en J. WOUTERS., "Het EU-cybersanctieregime en zijn verenigbaarheid met de grondrechten in het Unierecht", *RW* 2021-22, nr. 02, 11 september 2021, p.52.

———————————————————————-

Le régime des cyber-sanctions de l'UE de 2019 en réponse aux cyber-menaces et aux cyber-activités malveillantes.

Le 17 mai 2019, le Conseil de l'Union européenne (ci-après : le Conseil) a créé un cadre juridique pour répondre, par des mesures restrictives ciblées, à la tendance croissante des cyberattaques organisées ayant des conséquences import antes et constituant une menace extérieure pour l'Union ou ses États membres.[1]

Par exemple, le Conseil peut désormais imposer une interdiction de voyager[2] dans l'UE ou geler tous les fonds appartenant à des personnes physiques ou morales qui sont impliquées de quelque manière que ce soit dans des cyberattaques ou des tentatives de cyberattaques.[3] Ces mesures devraient avoir un effet dissuasif.

En outre, il convient de faire une distinction avec la responsabilité d'un État membre pour des faits de cyberattaque. L'application de mesures restrictives ciblées ne constitue pas une imposition de responsabilité, qui reste toujours une décision politique souveraine prise sur une base individuelle. Toutefois, chaque État membre est libre de déterminer la responsabilité d'un État tiers en matière

de cyberattaques.[4] Le législateur de l'Union souhaite ainsi éviter les difficultés juridiques, techniques et politiques liées à l'attribution d'une cyberattaque à un État.[5]

Par cyberattaque, le règlement du 17 mai 2019 entend l'une des activités suivantes :

– l'accès aux systèmes d'information ;

– perturbation des systèmes d'information ;

– perturbation des données ;

– interception des données.

Les cyberattaques qui constituent une menace externe comprennent celles ; qui ont pour origine ou sont menées par des entités situées en dehors de l'Union, qui utilisent des infrastructures situées en dehors de l'Union, qui sont menées par des personnes physiques ou morales basées ou opérant en dehors de l'Union, ou qui sont menées avec le soutien de personnes physiques ou morales opérant en dehors de l'Union.

Une cyberattaque peut donc constituer une menace pour un État membre si les systèmes d'information qui sont attaqués concernent, par exemple, des infrastructures critiques, ou des services nécessaires au maintien d'activités sociales et/ou économiques essentielles, ou des fonctions critiques de l'État telles que celles liées à la défense et à l'administration et au fonctionnement des institutions.[6]

Avec la cyberattaque de SolarWinds contre le gouvernement fédéral américain, la cyberattaque contre le parlement fédéral allemand en 2015 et la récente cyberattaque contre l'Agence européenne des médicaments de Pfizer et BioNTech, il est clair que la cybersécurité devient de plus en plus pertinente.[7] Déjà le 19 juin 2017, le Conseil adoptait des conclusions sur un cadre pour une réponse diplomatique conjointe aux cyberactivités malveillantes. Le dénommé « Instrumentarium pour la cyberdiplomatie », dans lequel le Conseil s'est dit préoccupé par la capacité et la volonté accrues des États et des acteurs non étatiques d'atteindre leurs objectifs par le biais de cyberattaques malveillantes. À l'époque, le Conseil soulignait déjà la nécessité croissante de protéger l'intégrité et la sécurité de l'Union, de ses États membres et de ses citoyens contre les cybermenaces.[8]

Conclusion

Comme décrit ci-dessus, avec le régime de cyber-punition, le législateur de l'Union choisit de sanctionner les acteurs non étatiques afin d'éviter les difficultés politiques et diplomatiques. Le régime des cyberpénalités exclut explicitement l'attribution de la responsabilité d'une cyberattaque à un État. Après tout, attribuer une cyberattaque à un État peut provoquer des tensions politiques considérables. La question est de savoir si le législateur de l'Union ne crée pas ainsi une fiction juridique. Après tout, la majorité des cyberattaques courantes sont menées à la demande ou avec le soutien des gouvernements, comme Stuxnet[9], Wannacry[10] et NotPetya[11] . En outre, l'apparence d'attribution à un État subsistera lorsque l'Union émettra des cyber-sanctions contre un ressortissant de cet État tiers particulier.[12]

Si vous avez des questions après avoir lu cet article, n'hésitez pas à nous contacter via l'adresse email joost.peeters@studio-legale.be ou par téléphone au 03 216 70 70.

[1] Voir le considérant (7) de la DÉCISION (PESC) 2019/797 du CONSEIL du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques menaçant l'Union ou ses États membres ; RÈGLEMENT (UE) 2019/796 du CONSEIL du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques menaçant l'Union ou ses États membres.

[2] Voir l'article 4 de la DÉCISION (PESC) 2019/797 du CONSEIL du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques menaçant l'Union ou ses États membres.

[3] Voir l'article 5 de la DÉCISION (PESC) 2019/797 du CONSEIL du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques menaçant l'Union ou ses États membres. Voir l'article 3 du RÈGLEMENT (UE) 2019/796 du Conseil du 17 mai 2019 concernant des mesures restrictives à l'encontre des cyberattaques qui menacent l'Union ou ses États membres.

[4] Voir les considérants (8) et (9) de la DÉCISION (PESC) 2019/797 du CONSEIL du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques menaçant l'Union ou ses États membres.

[5] A.VERHELST, M.RUELENS en J. WOUTERS., "Het EU-cybersanctieregime en zijn verenigbaarheid met de grondrechten in het Unierecht", *RW* 2021-22, nr. 02, 11 september 2021, p.52.

[6]
https://ecer.minbuza.nl/-/een-eu-cybersanctieregime-stap-voor-meer-veiligheid-in-cyberspace

[7] A.VERHELST, M.RUELENS en J. WOUTERS., “Het EU-cybersanctieregime en zijn verenigbaarheid met de grondrechten in het Unierecht”, *RW* 2021-22, nr. 02, 11 september 2021, p.43.

[8] Voir le considérant (1) de la DÉCISION (PESC) 2019/797 du CONSEIL du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques menaçant l’Union ou ses États membres.

[9] Les cyberattaques Stuxnet contre les installations nucléaires iraniennes étaient, selon certaines sources, une opération conjointe américano-israélienne. Voir DUMORTIER, V.PAPAKONSTANTINOU et P. DE HERT, “EU sanctions against cyber-attacks and defence rights : Wanna-Cry ?”, European Law Blog 2020, 2 et J. KAMBIC et S. LILES, “Non-State Cyber Power in ONG”, Journal of Information Warfare 2014, 57-67.

[10] WannaCry était une épidémie de ransomware qui visait le système d’exploitation Windows dans plusieurs pays. Voir Royaume-Uni, ministère des Affaires étrangères, ” Foreign Office Minister condems North Korean actor for WannaCry attacks “, communiqué de presse du 19 décembre 2019, disponible en ligne sur https://gov.uk/government/news/foreign-office-minister-condems-north-korean-actor-for-wannacry-attacks et G. FUSTER L. JASMONTAITE, ” Cybersecurity Regulation in the European Union : The Digital, the Critical and Fundamental Rights ” in M.CHRISTEN, B.GORDIJN and M.LOI (eds.), The Ethics of cybersecurity, Cham, Springer, 2020, 99-100.

[11] L’attaque NotPetya était une épidémie de ransomware qui visait à nouveau le système d’exploitation Windows. Voir Royaume-Uni, ministère des Affaires étrangères et Centre national de cybersécurité, ” Foreign Office Ministers condemns Russia for NotPetya attacks “, communiqué de presse du 15 février 2018 ; B. BLUMBERGS, K. VAN DER MEIJ et L.LINDSTRÖM, ” NotPetya and WannaCry Call for a Joint Response from International Community “, NATO Cooperative Cyber Defence Centre of Excellence Paper 2018.

[12] A.VERHELST, M.RUELENS en J. WOUTERS., “Het EU-cybersanctieregime en zijn verenigbaarheid met de grondrechten in het Unierecht”, *RW* 2021-22, nr. 02, 11 september 2021, p.52.

————————————————————————

Die EU-Cybersanktionsregelung 2019 als Reaktion auf Cyber-Bedrohungen und bösartige Cyber-Aktivitäten

Am 17. Mai 2019 hat der Rat der Europäischen Union (im Folgenden: Rat) einen Rechtsrahmen geschaffen, um mit gezielten restriktiven Maßnahmen auf den zunehmenden Trend zu organisierten Cyberangriffen mit erheblichen Folgen zu reagieren, die eine externe Bedrohung für die Union oder ihre Mitgliedstaaten darstellen.[1]

So kann der Rat nun beispielsweise ein Einreiseverbot[2] in die EU verhängen oder alle Gelder einfrieren, die natürlichen oder juristischen Personen gehören, die in irgendeiner Weise an Cyberangriffen oder versuchten Cyberangriffen beteiligt sind.[3] Solche Maßnahmen sollten abschreckend wirken.

Außerdem sollten sie von der Haftung eines Drittstaats für Cyberangriffe unterschieden werden. Die Anwendung gezielter restriktiver Maßnahmen kommt nicht der Auferlegung einer Haftung gleich, die immer eine souveräne politische Entscheidung auf individueller Basis bleibt. Es steht jedoch jedem Mitgliedstaat frei, die Haftung eines Drittstaates für Cyberangriffe festzulegen.[4] Auf diese Weise möchte der Unionsgesetzgeber die rechtlichen, technischen und politischen Schwierigkeiten vermeiden, die mit der Zuordnung eines Cyberangriffs zu einem Staat verbunden sind.[5]

Unter Cyberangriffen versteht die Verordnung vom 17. Mai 2019 eine der folgenden Aktivitäten:

– zugang zu Informationssystemen zu erhalten;

– unterbrechung von Informationssystemen;

– störende Daten;

– abfangen von Daten.

Zu den Cyberangriffen, die eine externe Bedrohung darstellen, gehören solche, die entweder von Einrichtungen außerhalb der Union ausgehen oder von diesen durchgeführt werden, Infrastrukturen außerhalb der Union nutzen oder von natürlichen oder juristischen Personen durchgeführt werden, die außerhalb der Union ansässig oder tätig sind, oder die mit Unterstützung von außerhalb der Union tätigen natürlichen oder juristischen Personen durchgeführt werden.

Ein Cyberangriff kann daher eine Bedrohung für einen Mitgliedstaat darstellen, wenn Informationssysteme angegriffen werden, die sich beispielsweise auf kritische Infrastrukturen oder Dienste beziehen, die für die Aufrechterhaltung wesentlicher sozialer und/oder wirtschaftlicher Aktivitäten oder kritischer Funktionen des Staates, z. B. im Zusammenhang mit der Verteidigung sowie der

Verwaltung und dem Funktionieren der Institutionen, erforderlich sind.[6]

Mit dem SolarWinds-Cyberangriff auf die US-Bundesregierung, dem Cyberangriff auf den deutschen Bundestag im Jahr 2015 und dem jüngsten Cyberangriff auf die Europäische Arzneimittelagentur von Pfizer und BioNTech wird deutlich, dass die Cybersicherheit zunehmend an Bedeutung gewinnt.[7] Bereits am 19. Juni 2017 hat der Rat Schlussfolgerungen zu einem Rahmen für eine gemeinsame diplomatische Reaktion auf bösartige Cyberaktivitäten angenommen. Das so genannte Instrumentarium für Cyber-Diplomatie, in dem der Rat seine Besorgnis über die zunehmende Fähigkeit und Bereitschaft von Staaten und nichtstaatlichen Akteuren zum Ausdruck brachte, ihre Ziele durch böswillige Cyber-Angriffe zu erreichen. Schon damals wies der Rat auf die wachsende Notwendigkeit hin, die Integrität und Sicherheit der Union, ihrer Mitgliedstaaten und ihrer Bürger vor Cyber-Bedrohungen zu schützen.[8]

Abschluss

Wie oben beschrieben, entscheidet sich der Unionsgesetzgeber bei der Cyber-Strafrechtsregelung für die Sanktionierung nichtstaatlicher Akteure, um politische und diplomatische Schwierigkeiten zu vermeiden. Die Cyber-Sanktionsregelung schließt ausdrücklich aus, dass einem Staat die Verantwortung für einen Cyber-Angriff zugeschrieben wird. Schließlich kann die Zuschreibung eines Cyberangriffs an einen Staat zu erheblichen politischen Spannungen führen. Es stellt sich die Frage, ob der Unionsgesetzgeber auf diese Weise nicht eine rechtliche Fiktion schafft. Schließlich wird die Mehrzahl der gängigen Cyberangriffe im Auftrag oder mit Unterstützung von Regierungen durchgeführt, wie z. B. Stuxnet[9], Wannacry[10] und NotPetya[11]. Darüber hinaus bleibt der Anschein der Zurechnung zu einem Staat bestehen, wenn die Union Cyber-Sanktionen gegen einen Staatsangehörigen dieses bestimmten Drittstaats verhängt.[12]

Wenn Sie nach der Lektüre dieses Artikels noch Fragen haben, zögern Sie bitte nicht, uns unter joost.peeters@studio-legale.be oder 03 216 70 70 zu kontaktieren.

[1] Siehe Erwägungsgrund (7) der BESCHLUSS (GASP) 2019/797 DES RATES vom 17. Mai 2019 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen; VERORDNUNG (EU) 2019/796 DES RATES vom 17. Mai 2019 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen.

[2] Siehe Artikel 4 der BESCHLUSS (GASP) 2019/797 DES RATES vom 17.

Mai 2019 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen.

[3] Siehe Artikel 5 der BESCHLUSS (GASP) 2019/797 DES RATES vom 17. Mai 2019 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen; Siehe Artikel 3 der VERORDNUNG (EU) 2019/796 DES RATES vom 17. Mai 2019 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen.

[4] Siehe Erwägungsgrund (7) und (8) der BESCHLUSS (GASP) 2019/797 DES RATES vom 17. Mai 2019 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen

[5] A.VERHELST, M.RUELENS en J. WOUTERS., "Het EU-cybersanctieregime en zijn verenigbaarheid met de grondrechten in het Unierecht", *RW* 2021-22, nr. 02, 11 september 2021, p.52.

[6]
https://ecer.minbuza.nl/-/een-eu-cybersanctieregime-stap-voor-meer-veiligheid-in-cyberspace

[7] A.VERHELST, M.RUELENS en J. WOUTERS., "Het EU-cybersanctieregime en zijn verenigbaarheid met de grondrechten in het Unierecht", *RW* 2021-22, nr. 02, 11 september 2021, p.43.

[8] Siehe Erwägungsgrund (1) der BESCHLUSS (GASP) 2019/797 DES RATES vom 17. Mai 2019 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen

[9] Die Stuxnet-Cyber-Angriffe auf iranische Atomanlagen waren einigen Quellen zufolge eine gemeinsame Operation der USA und Israels. Siehe DUMORTIER, V. PAPAKONSTANTINOU und P. DE HERT, "EU-Sanktionen gegen Cyberangriffe und Verteidigungsrechte: Wanna-Cry?", European Law Blog 2020, 2 und J. KAMBIC und S. LILES, "Non-State Cyber Power in ONG", Journal of Information Warfare 2014, 57-67.

[10] WannaCry war ein Ausbruch von Ransomware, die in mehreren Ländern auf das Windows-Betriebssystem abzielte. Siehe UK, Department of Foreign Affairs, "Foreign Office Minister condemns North Korean actor for WannaCry attacks", Pressemitteilung vom 19. Dezember 2019, online verfügbar unter https://gov.uk/government/news/foreign-office-minister-condems-north-korean-actor-for-wannacry-attacks und G. FUSTER L. JASMONTAITE, "Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental

Rights" in M.CHRISTEN, B.GORDIJN and M.LOI (eds.), The Ethics of cybersecurity, Cham, Springer, 2020, 99-100.

[11] De NotPetya-aanval was een uitbraak van ransomware die opnieuw het Windowsbesturingssysteem viseerde. Zie VK, Departement van Buitenlandse Zaken en Nationaal Centrum voor Cyberbeveiliging, "Foreign Office Ministers condems Russia for NotPetya attacks", Nieuwsmededeling 15 februari 2018; B. BLUMBERGS, K. VAN DER MEIJ en L.LINDSTRÖM, "NotPetya and WannaCry Call for a Joint Response from International Community", NATO Cooperative Cyber Defence Centre of Excellence Paper 2018.

[12] A.VERHELST, M.RUELENS en J. WOUTERS., "Het EU-cybersanctieregime en zijn verenigbaarheid met de grondrechten in het Unierecht", *RW* 2021-22, nr. 02, 11 september 2021, p.52.

————————————————–

The 2019 EU cyber sanctions regime in response to cyber threats and malicious cyber activities

On 17 May 2019, the Council of the European Union (hereinafter: Council) created a legal framework to respond with targeted restrictive measures to the increasing trend of organised cyber-attacks with significant consequences that pose an external threat to the Union or its Member States.[1]

For example, the Council can now impose a ban on travelling[2] to the EU or freeze all funds belonging to natural or legal persons who are in any way involved in cyber-attacks or attempted cyber-attacks.[3] Such measures should serve as a deterrent.

Moreover, they should be distinguished from holding a member state liable for a cyber-attack. The application of targeted restrictive measures does not imply liability, which always remains a sovereign political decision taken on an individual basis. However, each Member State is free to determine the liability of a third State in respect of cyber-attacks.[4] In this way, the Union legislator wishes to avoid the legal, technical and political difficulties of attributing a cyber-attack to a State.[5]

By cyber-attacks, the regulation of 17 May 2019 means one of the following activities:

– gaining access to information systems;

– disrupting information systems;

– disrupting data;

– intercepting data.

Cyber-attacks that pose an external threat include those that either originate from, or are conducted by, entities outside the Union, use infrastructure located outside the Union, or are conducted by natural or legal persons based or operating outside the Union, or are conducted with the support of natural or legal persons operating outside the Union.[6]

A cyber-attack may therefore pose a threat to a Member State if information systems are attacked which, for example, relate to critical infrastructure, or services necessary for the maintenance of essential social and/or economic activities, or critical functions of the state such as those relating to defence and the administration and functioning of the institutions.

With the SolarWinds cyber-attack on the US federal government, the cyber-attack on the German federal parliament in 2015 and the recent cyber-attack on the European Medicines Agency of Pfizer and BioNTech, it is clear that cyber security is becoming increasingly relevant.[7] Already on 19 June 2017, the Council adopted conclusions on a framework for a joint diplomatic response to malicious cyber activities. The so-called Instrumentarium for Cyber Diplomacy in which the Council expressed her concerns about the increased capacity and willingness of States and non-state actors to achieve their objectives through malicious cyber-attacks. At the time, the Council was already highlighting the growing need to protect the integrity and security of the Union, its Member States and its citizens from cyber threats.[8]

Conclusion

As described above, with the cyber-sanctions regime, the Union legislator chooses to sanction non-state actors in order to avoid political and diplomatic difficulties. The cyber-sanctions regime explicitly excludes attributing responsibility for a cyber-attack to a state. After all, attributing a cyber-attack to a state can cause considerable political tensions. The question is whether the Union legislator is not creating a legal fiction in this way. After all, the majority of common cyber-attacks are carried out at the request or with the support of governments, such as Stuxnet[9], Wannacry[10] and NotPetya[11]. Moreover, the appearance of attribution to a State will remain when the Union issues cyber-sanctions against a citizen of that particular third State.[12]

We will closely monitor the evolution in this area. If you have any questions after reading this article, please do not hesitate to contact us at joost.peeters@studio-legale.be or 03 216 70 70.

[1] See recital (7) of the COUNCIL DECISION (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States; COUNCIL REGULATION (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

[2] See article 4 of the COUNCIL DECISION (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

[3] See article 5 of the COUNCIL DECISION (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States; See article 3 of the COUNCIL REGULATION (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

[4] See recital (8) and (9) of the COUNCIL DECISION (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

[5] A.VERHELST, M.RUELENS en J. WOUTERS., "Het EU-cybersanctieregime en zijn verenigbaarheid met de grondrechten in het Unierecht", *RW* 2021-22, nr. 02, 11 september 2021, p.52.

[6]
https://ecer.minbuza.nl/-/een-eu-cybersanctieregime-stap-voor-meer-veiligheid-in-cyberspace

[7] A.VERHELST, M.RUELENS en J. WOUTERS., "Het EU-cybersanctieregime en zijn verenigbaarheid met de grondrechten in het Unierecht", *RW* 2021-22, nr. 02, 11 september 2021, p.43.

[8] See recital (1) of the COUNCIL DECISION (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

[9] The Stuxnet cyber-attacks against Iranian nuclear facilities were, according to some sources, a joint US-Israeli operation. See DUMORTIER, V.PAPAKONSTANTINOU and P. DE HERT, "EU sanctions against cyber-attacks

and defence rights: Wanna-Cry?", European Law Blog 2020, 2 and J. KAMBIC and S. LILES, "Non-State Cyber Power in ONG", Journal of Information Warfare 2014, 57-67.

[10] WannaCry was an outbreak of ransomware that targeted the Windows operating system in several countries. See UK, Department of Foreign Affairs, "Foreign Office Minister condems North Korean actor for WannaCry attacks", Press release 19 December 2019, available online at https://gov.uk/government/news/foreign-office-minister-condems-north-korean-actor-for-wannacry-attacks and G. FUSTER L. JASMONTAITE, "Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights" in M.CHRISTEN, B.GORDIJN and M.LOI (eds.), The Ethics of cybersecurity, Cham, Springer, 2020, 99-100.

[11] The NotPetya attack was an outbreak of ransomware that again targeted the Windows operating system. See UK, Department of Foreign Affairs and National Cyber Security Centre, "Foreign Office Ministers condemns Russia for NotPetya attacks", News Release 15 February 2018; B. BLUMBERGS, K. VAN DER MEIJ and L.LINDSTRÖM, "NotPetya and WannaCry Call for a Joint Response from International Community", NATO Cooperative Cyber Defence Centre of Excellence Paper 2018.

[12] A.VERHELST, M.RUELENS en J. WOUTERS., "Het EU-cybersanctieregime en zijn verenigbaarheid met de grondrechten in het Unierecht", *RW* 2021-22, nr. 02, 11 september 2021, p.52.