Tribunal fédéral – 4A_206/2023
Ire Cour de de droit civil
Arrêt du 17 août 2023

Assurances privées

Exclusion de couverture, interprétation de la clause de sanction, principe de la confiance

Art. 18 CO

Une société cotée en bourse a été victime d'une cyberattaque bien connue qui consiste à crypter les fichiers, notamment les données clients, de sorte que ces fichiers ne peuvent plus être lus. Seul le code de décryptage, connu des cyberattaquants, permet de décrypter les données. En l'espèce, une rançon de 1'500 bitcoins était demandée pour la remise du code de décryptage. Cette rançon a été payée par la société victime de cette attaque (c. A).

La société demande ensuite la couverture de son dommage à son assureur, qui refuse de le couvrir en invoquant une exclusion de couverture. **Selon la clause invoquée, l'assurance serait libérée de son obligation de paiement si le paiement de la somme assurée contrevient notamment au droit américain des sanctions.** Le paiement de la somme demandée contreviendrait, selon l'assurance, au droit américain des sanctions car l'attaque aurait été proférée par des cyberattaquants russes inscrits sur la « *Specially Designated Nationals and Blocked Persons-List* » (liste SDN) du « *U.S. Treasury Department's Office of Foreign Assets Controls* » (OFAC) (c. A). La liste SDN contient des entreprises, des organisations et des individus qui ont été identifiés comme constituant une menace pour la sécurité nationale et la politique étrangère et économique des États-Unis. Leurs avoirs sont bloqués et il est généralement interdit aux ressortissants américains de traiter avec eux (https://ofac.treasury.gov/specially-designated-nationals-list-data-formats-data-schemas).

Le *Handelsgericht* de Zurich admet la demande en paiement déposée par la société en raison du fait qu'il serait hautement improbable que l'assureur soit sanctionné par l'OFAC en cas de paiement de la somme assurée. Cela rendrait la clause de sanction inapplicable. En effet, l'assureur n'est pas parvenu à prouver que l'attaque était le fait des cyberattaquants russes inscrits sur la liste américaine précitée et que cette société aurait profité financièrement de l'attaque (c. B). L'assureur dépose un recours en matière civile au TF à l'encontre du jugement du « *Handelsgericht* » de Zurich (c. C).

Le recours est rejeté par le TF qui confirme l'appréciation du tribunal zurichois. En effet, l'assurance n'a pas été en mesure de prouver que les cyberattaquants russes, sanctionnés par le gouvernement américain étaient les auteurs de la cyberattaque contre la société ou qu'ils en ont profité. Il manque donc un point de rattachement au droit américain des sanctions. Une sanction de l'assurance en cas de versement de la somme assurée à la société pour violation du droit américain des sanctions est hautement improbable. Le TF confirme ainsi que la clause de sanction invoquée par l'assurance ne s'applique pas (c. 5). De plus, **il interprète la clause de sanction et considère qu'il faut un risque de sanction pour violation du droit américain des sanctions, ce qui n'est pas le cas en l'espèce** (c. 6). A cela s'ajoute que **le simple fait que le logiciel utilisé proviendrait des cyberattaquants russes inscrits sur la liste SDN ne suffit pas à prouver l'existence d'un lien entre les cyberattaquants russes et la cyberattaque contre la société, ce qui serait insuffisant pour appliquer la clause de sanction** (c. 7.1.1. et 7.1.4.). Pour finir, le TF relève que l'assurance ne peut pas se plaindre du fait qu'un droit étranger, soit le droit américain en l'espèce, n'a pas été correctement appliqué (art. 96 let. b LTF). Seul l'arbitraire et la violation de l'art. 9 Cst. dans son application peuvent être invoqués (c. 7.2.1.).

Note : Il s'agit, à notre connaissance, du premier arrêt du TF relatif au paiement d'une rançon suite à une cyberattaque dans le domaine du droit des assurances privées.

Auteure : Corinne Monnard Séchaud, avocate à Lausanne

Beschwerde gegen das Urteil des Handelsgerichts des Kantons Zürich vom 9. März 2023 (HG210017-O).

Sachverhalt:

A.

A.a. Die B. Ltd. (Klägerin, Beschwerdegegnerin) mit Sitz in U. (Schweiz) ist die börsenkotierte Holdinggesellschaft der weltweit tätigen B.-Gruppe, die namentlich Geräte zur xxx entwickelt, herstellt und vertreibt. Die A. Limited (Beklagte, Beschwerdeführerin) ist eine in Grossbritannien registrierte Versicherung mit Sitz in V. (Grossbritannien). Sie betreibt das Versicherungsgeschäft hauptsächlich in London, Singapur, Miami und New York. Seit 2018 wird die Beklagte zu 100 % von der C. Inc., einer nach US-amerikanischem Recht organisierten Gesellschaft, indirekt gehalten und kontrolliert.

A.b. Am tt.mm.Tatjahr wurde die Klägerin Opfer einer Cyber-Erpressung unter Verwendung der Ransomware (Schadsoftware) D.. Diese verschlüsselte Dateien (u.a. auch Kundendaten) auf den klägerischen Systemen, sodass die Dateien nicht mehr gelesen werden konnten. Die Klägerin sah sich gezwungen, den Betrieb ihrer Callcenter, Webseiten und einiger Online-Dienste einzustellen. Ein Dechiffriercode (um die verschlüsselten Dateien wieder verwenden zu können) wurde von den Angreifern erst nach Zahlung eines Lösegelds in Höhe von 1'500 Bitcoins in Aussicht gestellt. Die Klägerin beauftragte das US-amerikanische Unternehmen E. LLC, das Lösegeld in Bitcoins zu bezahlen. Am tt.mm.Tatjahr waren die klägerischen Systeme wieder operabel. Aus dem Angriff erwuchs der Klägerin ein Schaden von ca. yyy Millionen USD.

A.c. Die Klägerin ist gegen Cyberangriffe versichert, wobei die Beklagte Mitversicherin der Police ist. Gemäss der Police ist jede Versicherung gemeinsam mit den anderen, aber nicht solidarisch für ihren gezeichneten Anteil leistungspflichtig. Die Beklagte verweigert als Einzige die Zahlung. Sie beruft sich auf einen in der Police enthaltenen Deckungsausschluss (Sanktionsklausel). Gemäss dieser wird die Versicherung von ihrer Zahlungspflicht befreit, wenn die Zahlung der Versicherungssumme namentlich gegen das US-amerikanische Sanktionsrecht verstösst.
Unstrittig ist, dass die von der Beklagten für den Cyberangriff verantwortlich gemachte cyber-kriminelle russische Gruppe F. vom "Office of Foreign Assets Control" (OFAC) des US-amerikanischen Finanzministeriums sanktioniert und auf die "Specially Designated Nationals and Blocked Persons-List" (SDN-Liste) gesetzt worden ist. Die Beklagte stellt sich auf den Standpunkt, sie würde im Falle einer Auszahlung der Versicherungsleistung an die Klägerin das US-amerikanische Sanktionsrecht verletzen.

B.
Mit Klage vom 25. Januar 2021 beantragte die Klägerin beim Handelsgericht des Kantons Zürich, es seien die Beklagten (sic) zu verpflichten, ihr USD 987'098.-- nebst Zins zu bezahlen.
Mit Urteil vom 9. März 2023 hiess das Handelsgericht die Klage gut und verpflichtete die Beklagte, der Klägerin USD 987'098.-- nebst Zins zu bezahlen.
Es erwog, die Beklagte vermöge nicht nachzuweisen, dass die von der US-amerikanischen Regierung sanktionierte F. Urheberin des Cyberangriffs gewesen sei bzw. vom Cyberangriff profitiert und damit ein Interesse im Sinne des US-amerikanischen Sanktionsrechts daran gehabt habe. Damit bestehe kein Anknüpfungspunkt zum US-amerikanischen Sanktionsrecht und eine Bestrafung der Beklagten bei Auszahlung der Versicherungssumme sei höchst unwahrscheinlich, womit die Sanktionsklausel keine Anwendung finde.

C.
Mit Beschwerde in Zivilsachen beantragt die Beklagte dem Bundesgericht, es sei das Urteil des Handelsgerichts aufzuheben und die Klage abzuweisen. Eventualiter sei die Sache zur Neubeurteilung an das Handelsgericht zurückzuweisen, wobei dieses anzuweisen sei, ein gerichtliches Gutachten zur Frage einzuholen, ob die Ransomware D. der F. zuzurechnen sei. Die Beschwerdegegnerin beantragt, die Beschwerde abzuweisen, soweit darauf einzutreten ist. Die Vorinstanz hat auf Vernehmlassung verzichtet. Die Parteien haben unaufgefordert repliziert und dupliziert.
Mit Präsidialverfügung vom 16. Mai 2023 wurde der Beschwerde antragsgemäss die aufschiebende Wirkung erteilt.

Erwägungen:

1.

1.1. Das Bundesgericht wendet das Recht von Amtes wegen an (Art. 106 Abs. 1 BGG). Es prüft aber unter Berücksichtigung der allgemeinen Begründungsanforderungen (Art. 42 Abs. 1 und 2 BGG) grundsätzlich nur die geltend gemachten Rügen, sofern die rechtlichen Mängel nicht geradezu offensichtlich sind. Es ist nicht gehalten, wie eine erstinstanzliche Behörde alle sich stellenden rechtlichen Fragen zu untersuchen, wenn diese vor Bundesgericht nicht mehr vorgetragen werden (BGE 140 III 86 E. 2, 115 E. 2). Die Beschwerde ist dabei hinreichend zu begründen, andernfalls wird darauf nicht eingetreten. Unerlässlich ist im Hinblick auf Art. 42 Abs. 2 BGG, dass die Beschwerde auf die Begründung des angefochtenen Entscheids eingeht und im Einzelnen aufzeigt, worin eine Verletzung von Bundesrecht liegt. Die beschwerdeführende Partei soll in der Beschwerdeschrift nicht bloss die Rechtsstandpunkte, die sie im kantonalen Verfahren eingenommen hat, erneut bekräftigen, sondern mit ihrer Kritik an den als rechtsfehlerhaft erachteten Erwägungen der Vorinstanz ansetzen (vgl. BGE 134 II 244 E. 2.1).

1.2. Soweit ein Entscheid auf mehreren selbstständigen alternativen Begründungen beruht, ist für jede einzelne darzutun, weshalb sie Recht verletzt; denn soweit nicht beanstandete Begründungen das angefochtene Urteil selbstständig stützen, fehlt das Rechtsschutzinteresse an der Beurteilung der gehörig begründeten Rügen (BGE 133 IV 119 E. 6.3; vgl. auch BGE 132 III 555 E. 3.2; je mit Hinweisen).

1.3. Die Begründung hat in der Beschwerdeschrift selbst zu erfolgen. Die beschwerdeführende Partei darf eine allfällige Replik nicht dazu verwenden, ihre Beschwerde zu ergänzen oder zu verbessern. Zulässig sind nur Vorbringen, zu denen erst die Ausführungen in der Vernehmlassung eines anderen Verfahrensbeteiligten Anlass geben (vgl. BGE 135 I 19 E. 2.2; 132 I 42 E. 3.3.4).

2.
Das Bundesgericht legt seinem Urteil den Sachverhalt zugrunde, den die Vorinstanz festgestellt hat (Art. 105 Abs. 1 BGG). Dazu gehören sowohl die Feststellungen über den streitgegenständlichen Lebenssachverhalt als auch jene über den Ablauf des vor- und erstinstanzlichen Verfahrens, also die Feststellungen über den Prozesssachverhalt (BGE 140 III 16 E. 1.3.1 mit Hinweisen). Es kann die Sachverhaltsfeststellung der Vorinstanz nur berichtigen oder ergänzen, wenn sie offensichtlich unrichtig ist oder auf einer Rechtsverletzung im Sinne von Art. 95 BGG beruht (Art. 105 Abs. 2 BGG). "Offensichtlich unrichtig" bedeutet dabei "willkürlich" (BGE 140 III 115 E. 2, 264 E. 2.3). Überdies muss die Behebung des Mangels für den Ausgang des Verfahrens entscheidend sein können (Art. 97 Abs. 1 BGG).

Für eine Kritik am festgestellten Sachverhalt gilt das strenge Rügeprinzip von Art. 106 Abs. 2 BGG (BGE 140 III 264 E. 2.3 mit Hinweisen). Die Partei, welche die Sachverhaltsfeststellung der Vorinstanz anfechten will, muss klar und substanziiert aufzeigen, inwiefern die genannten Voraussetzungen erfüllt sein sollen (BGE 140 III 16 E. 1.3.1 mit Hinweisen). Wenn sie den Sachverhalt ergänzen will, hat sie zudem mit präzisen Aktenhinweisen darzulegen, dass sie entsprechende rechtsrelevante Tatsachen und taugliche Beweismittel bereits bei den Vorinstanzen prozesskonform eingebracht hat (BGE 140 III 86 E. 2). Genügt die Kritik diesen Anforderungen nicht, können Vorbringen mit Bezug auf einen Sachverhalt, der vom angefochtenen Entscheid abweicht, nicht berücksichtigt werden (BGE 140 III 16 E. 1.3.1).

3.
Der Anspruch auf rechtliches Gehör (Art. 29 Abs. 2 BV) verlangt insbesondere, dass die Gerichte die rechtserheblichen Vorbringen der Parteien anhören und bei der Entscheidfindung berücksichtigen (BGE 136 I 184 E. 2.2.1; 134 I 83 E. 4.1). Damit sich die Parteien ein Bild über die Erwägungen des Gerichts machen können, ist sein Entscheid zu begründen. Die Begründung muss kurz die Überlegungen nennen, von denen sich das Gericht hat leiten lassen und auf die sich sein Entscheid stützt (BGE 142 III 433 E. 4.3.2; 136 I 184 E. 2.2.1). Nicht erforderlich ist hingegen, dass sich der Entscheid mit allen Parteistandpunkten einlässlich auseinander setzt und jedes einzelne Vorbringen ausdrücklich widerlegt. Es genügt, wenn der Entscheid gegebenenfalls sachgerecht angefochten werden kann (BGE 142 III 433 E. 4.3.2; 141 III 28 E. 3.2.4; je mit Hinweisen).

4.
Die Police enthält folgende Klausel:

" SANCTION LIMITATION AND EXCLUSION CLAUSE
No (re) insurer shall be deemed to provide cover and no (re) insurer shall be liable to pay any claim or provide any benefit hereunder to the extent that the provision of such cover, payment of such claim or provision of such benefit would expose that (re) insurer to any sanction, prohibition or restriction under United Nations resolutions or the trade or economic sanctions, laws or regulations of the European Union, United Kingdom or United States of America. "

5.
Die Vorinstanz erwog, die Parteien hätten in der Police gültig die Gerichte des Kantons Zürich als zuständig und Schweizer Recht für anwendbar erklärt. Die Police erfasse unbestritten den Schaden aus dem Cyberangriff vom tt.mm.Tatjahr. Die Beschwerdeführerin habe nicht auf die Einrede der Sanktionsklausel verzichtet. Ebenso wenig sei diese als ungewöhnlich zu qualifizieren.
Nach US-amerikanischem Sanktionsrecht gelte die Beschwerdeführerin als sog. "non-U.S.-Person". Eine "non-U.S.-Person" könne wegen Verstosses gegen das Sanktionsrecht bestraft werden, wenn sie einen Verstoss durch eine "U.S.-Person" verursache. Ein solcher Verstoss könne namentlich darin liegen, dass eine Zahlung in USD erfolge, weil im Rahmen des Clearing und Settlements der Zahlung zwingend ein US-amerikanischer Finanzdienstleister an der Transaktion beteiligt werde. Voraussetzung für einen Verstoss sei allerdings, dass ein Interesse ("property or interests in property") einer sanktionierten Person (SDN) berührt werde. Die blosse Urheberschaft betreffend eine Ransomware stelle kein solches Interesse dar. Hingegen qualifiziere ein Profit einer sanktionierten Person im Zusammenhang mit einer Lösegeldzahlung als ein solches Interesse im Sinne des US-amerikanischen Sanktionsrechts. Dieses Interesse erfasse auch eine Versicherungsleistung, die den Schaden aus der Lösegeldzahlung ersetze, unabhängig davon, ob die Versicherungsleistung an die sanktionierte Person oder an den Versicherungsnehmer ausbezahlt werde.

Das Beweismass richte sich grundsätzlich nach der lex causae. Vorliegend sei indes zu berücksichtigen, dass einzuschätzen sei, ob das OFAC angesichts des erstellten Sachverhalts annähme, eine sanktionierte Person (SDN) stehe hinter dem Cyberangriff auf die Beschwerdegegnerin. Insofern ergebe sich letztlich das anzuwendende Beweismass aus dem vertraglichen Verweis auf das US-amerikanische Recht. Die Parteiengutachter seien sich einig, dass die Verletzung von Sanktionen mit einer "preponderance of reliable, probative and substantial evidence" erstellt sein müsse, damit das OFAC Massnahmen anordnen könne.
Die Beschwerdeführerin vermöge nicht nachzuweisen, dass die von der US-amerikanischen Regierung sanktionierte F. Urheberin des Cyberangriffs gegen die Beschwerdegegnerin gewesen sei bzw. davon profitiert habe. Es fehle somit ein Anknüpfungspunkt zum US-amerikanischen Sanktionsrecht und eine Bestrafung der Beschwerdeführerin bei Auszahlung der Versicherungssumme an die Beschwerdegegnerin wegen Verstosses gegen das US-amerikanische Sanktionsrecht sei höchst unwahrscheinlich. Entsprechend greife die von ihr angerufene Sanktionsklausel nicht.

6.
Umstritten ist die Auslegung der Sanktionsklausel.

6.1. Die Beschwerdeführerin rügt, die Vorinstanz halte bei der Auslegung der Sanktionsklausel rechtsfehlerhaft fest, "dass die sanktionierende Behörde eine konkrete ' sanction, prohibition or restriction ' anordnen muss, damit die Einrede der Sanktionsklausel erfolgreich erhoben werden kann". Die Vorinstanz weiche damit in rechtswidriger Weise vom Wortlaut der Klausel ab, da diese keineswegs verlange, dass eine Sanktion angeordnet werden müsse.

6.1.1. Die Vorinstanz erwog, eine Auslegung nach dem Vertrauensprinzip erhelle, dass ein erhebliches Risiko einer Bestrafung durch das OFAC im Sinne der Sanktionsklausel dann bestehe, wenn eine überwiegende Wahrscheinlichkeit dafür spreche, dass das OFAC in Kenntnis des Sachverhalts und gestützt auf das US-amerikanische Cyber-Sanktionsrecht nicht nur ein Enforcement-Verfahren gegen die Beschwerdeführerin einleiten würde, sondern diese im Anschluss an das Enforcement-Verfahren wegen Verstosses gegen das US-amerikanische Sanktionsrecht bestrafen würde.

6.1.2. Wie sich aus den obigen vorinstanzlichen Erwägungen ohne Weiteres ergibt, meinte die Vorinstanz mit der von der Beschwerdeführerin beanstandeten Formulierung nicht, dass die betreffende Klausel nur dann greift, wenn tatsächlich (bereits) eine Sanktion erfolgte. Dies ergibt sich bereits daraus, dass die Vorinstanz am Ende des betreffenden Abschnitts ausführt, einem Risiko ernsthaft ausgesetzt zu sein, bedeute somit nicht, dass sich das Risiko tatsächlich oder gar endgültig (im Sinne von rechtskräftig) verwirklichen müsse. Vielmehr ging es der Vorinstanz in der von der Beschwerdeführerin beanstandeten Stelle darum, darzulegen, dass das blosse Risiko der Einleitung eines Enforcement-Verfahrens nicht ausreicht, sondern dass es eines Risikos einer Bestrafung wegen Verstosses gegen das US-amerikanische Sanktionsrecht bedürfe.

7.
Umstritten ist weiter, ob die Vorinstanz zu Recht davon ausgegangen ist, eine Bestrafung der Beschwerdeführerin wegen Verstosses gegen das US-amerikanische Sanktionsrecht im Falle der Auszahlung der Versicherungssumme an die Beschwerdegegnerin sei höchst unwahrscheinlich.

7.1.

7.1.1. Die Vorinstanz erwog, einen direkten Nachweis der Beteiligung der F. am Cyberangriff offeriere die Beschwerdeführerin nicht. Sie stütze ihre Behauptungen vielmehr auf Indizienbeweise. Kern ihrer Argumentation sei dabei die Annahme, dass sich die Beteiligung der F. am Angriff gegen die Beschwerdegegnerin aus der (behaupteten) Urheberschaft der F. betreffend den Programmcode von D. und den beim Angriff beobachteten Modus Operandi ableiten lasse. Sie wolle die Urheberschaft der F. betreffend den Programmcode von D. anhand eines Vergleichs der beim Angriff verwendeten Ransomware D. mit den älteren Ransomwares G., H. und I. nachweisen, die aus ihrer Sicht alle der F. zuzuschreiben seien.
Weder in den Rechtsschriften noch in den Gutachten würden die Programmcodes der verschiedenen Ransomwares näher dargestellt. Die Beschwerdeführerin behaupte zwar einige Übereinstimmungen zwischen den Ransomwares sowie der Modi Operandi. Es bleibe aber bei unsubstanziierten Behauptungen. Insbesondere fehle es an konkreten Ausführungen zum Cyberangriff auf die Beschwerdegegnerin. Die Behauptung einer gewissen "Verwandtschaft" zwischen den verschiedenen Programmcodes der betreffenden Ransomwares genüge nicht, um einen sanktionsrelevanten Konnex zwischen der F. und dem Cyberangriff gegen die Beschwerdegegnerin nachzuweisen. Nicht auszuschliessen sei, dass andere Nutzer einen Programmcode der F. für die Entwicklung ihrer eigenen Ransomware verwendet hätten, ohne Wissen derselben. Entsprechend vermöchte der Nachweis der blossen Urheberschaft der F. betreffend den Programmcode von D. für sich allein noch kein Interesse einer sanktionierten Person (SDN) im Sinne des US-amerikanischen Sanktionsrechts darzutun. Der Vergleich der Programmcodes basiere nämlich auf der Prämisse, dass die Ransomwares - auch nachdem sie bereits im Umlauf seien - exklusiv von derjenigen Gruppe eingesetzt und weiterentwickelt würden, die sie auch ursprünglich programmiert haben. Sie habe aber nicht aufgezeigt, dass neuere Ransomwares, deren Programmcode Ähnlichkeiten mit dem Programmcode einer früher zirkulierenden, älteren Ransomware aufweise, nur bzw. stets von derselben Gruppe entwickelt und eingesetzt würden, die die ältere Ransomware programmiert habe. Die Prämisse der Beschwerdeführerin bleibe unbewiesen.

7.1.2. Das OFAC habe zudem nie dargelegt, aufgrund welcher Tatsachen es die cyberkriminellen Gruppen identifiziere, sondern diese jeweils ohne Veröffentlichung der eigenen forensischen Abklärungen in die SDN-Liste aufgenommen. Die Kriterien einer Zuordnung von einzelnen Cyberangriffen zu bestimmten Gruppen bleibe unbekannt. Die Ausführungen des OFAC, dass die F. Lösegeldzahlungen von über 100 Millionen Dollar erpresst habe, liessen darauf schliessen, dass es gestützt auf konkrete Zahlungsflüsse die F. als Täterin identifiziert habe und die Zuordnung einzelner Cyberangriffe zu einer SDN insbesondere auch anhand der Zahlungsflüsse erfolge. Die Urheberschaft hinsichtlich einer Ransomware möge zwar Grundlage für die Aufnahme in die SDN-Liste sein. Aber sie stelle für sich allein kein Interesse einer SDN im Sinne des US-amerikanischen Sanktionsrechts dar; ebenso wenig lasse sich allein gestützt darauf ein bestimmter Cyberangriff einer bestimmten Gruppierung zuordnen.

7.1.3. Auch das bisherige Verhalten des OFAC bezüglich des Cyberangriffs sei als gewichtiger Faktor zu berücksichtigen. Das OFAC habe bis heute weder gegen die Beschwerdegegnerin (oder eine mit dieser verbundenen US-Gesellschaft) noch gegen die mit der Lösegeldzahlung beauftragten E. LLC ein Enforcement-Verfahren durchgeführt. Auch gegen die anderen Versicherungen, die im Zusammenhang mit dem Cyberangriff Leistungen an die Beschwerdegegnerin erbracht hätten, seien

(soweit bekannt) keine Enforcement-Verfahren durchgeführt oder gar Strafen ausgesprochen worden.

7.1.4. Die Beweisführung der Beschwerdeführerin scheitere damit bereits in ihrem Ansatz. Die blosse Urheberschaft der F. hinsichtlich der Ransomware D. würde (wenn sie denn überhaupt nachgewiesen wäre) nicht ausreichen, um die Sanktionsklausel zu aktivieren. In einer Eventualbegründung legte die Vorinstanz schliesslich dar, dass die Beschwerdeführerin auch nicht die Urheberschaft der F. betreffend den Programmcode von D. nachzuweisen vermöge.

7.2. Die Beschwerdeführerin macht in ihrer Beschwerde geltend, die Vorinstanz gehe unzutreffend davon aus, der Nachweis der Urheberschaft der F. betreffend den Programmcode von D. begründe für sich allein kein Interesse der F. im Sinne des US-amerikanischen Sanktionsrechts. Die Vorinstanz verneine ein solches Interesse der F. unter Verletzung ihres Anspruchs auf rechtliches Gehör.

7.2.1. Da der Entscheid eine vermögensrechtliche Sache betrifft, kann nicht gerügt werden, das ausländische Recht - vorliegend das US-amerikanische Sanktionsrecht - sei nicht richtig angewendet worden (Art. 96 lit. b BGG), sondern ausschliesslich, die Anwendung sei willkürlich und verstosse gegen Art. 9 BV (BGE 135 III 670 E. 1.4; 133 III 446 E. 3.1; Urteile 4A_659/2020 vom 6. August 2021 E. 3.3; 4A_351/2019 vom 18. Februar 2020 E. 3.1.1).

7.2.2. Nach ständiger Rechtsprechung des Bundesgerichts liegt Willkür in der Rechtsanwendung vor, wenn der angefochtene Entscheid offensichtlich unhaltbar ist, mit der tatsächlichen Situation in klarem Widerspruch steht, eine Norm oder einen unumstrittenen Rechtsgrundsatz krass verletzt oder in stossender Weise dem Gerechtigkeitsgedanken zuwiderläuft. Das Bundesgericht hebt einen Entscheid jedoch nur auf, wenn nicht bloss die Begründung, sondern auch das Ergebnis unhaltbar ist. Dass eine andere Lösung ebenfalls als vertretbar oder gar zutreffender erscheint, genügt nicht (BGE 144 I 113 E. 7.1; 142 II 369 E. 4.3; je mit Hinweisen).

7.2.3. Die Beschwerdeführerin vermag nicht darzutun, dass es offensichtlich unhaltbar wäre, wenn die Vorinstanz davon ausgeht, allein der Nachweis der blossen Urheberschaft der F. betreffend den Programmcode von D. vermöge für sich allein kein Interesse einer SDN im Sinne des US-amerikanischen Sanktionsrechts darzutun. Die Beschwerdeführerin tut namentlich nicht dar, dass es im Ergebnis unhaltbar ist, wenn die Vorinstanz (unter der Annahme, die Urheberschaft betreffend den Programmcode der Ransomware D. sei durch den Vergleich mit älteren Ransomwares erstellt) nicht davon ausgeht, jeder Einsatz von D. - auch derjenige durch Dritte - stelle ein Interesse der F. nach US-amerikanischem Sanktionsrecht dar, weil diese auf jeden Fall finanziell davon profitiere.
Entgegen der Beschwerdeführerin hat die Vorinstanz damit auch nicht ihre Begründungspflicht verletzt oder ist vom aktenmässig erstellten Sachverhalt abgewichen. Aus dem Umstand, dass gemäss dem Bericht des Experten der Beschwerdegegnerin Ransomware an interessierte Parteien zur massenhaften Verbreitung verkauft wird ("commodity malware is typically sold to interested parties for mass distribution [...]"), musste die Vorinstanz (entgegen der Beschwerdeführerin) bereits nicht zwingend ableiten, dass die F. bei jedem Einsatz der Ransomware D. finanziell profitiert (entgeltliches Zurverfügungstellen der Ransomware D.). Die Annahme, dass die Ransomware durch gewisse Nutzer auch unentgeltlich übernommen werden kann, schliesst das Bestehen eines Marktes für den Verkauf von Ransomware nicht ohne Weiteres aus. Damit geht das Argument der Beschwerdeführerin fehl, mit der vorinstanzlichen Annahme bestünde gar kein Markt, um Ransomware verkaufen zu können.

Selbst wenn man mit der Beschwerdeführerin davon ausgehen möchte, dass die F. bei jedem Einsatz der Ransomware D. finanziell profitiert, wäre es nicht willkürlich, wenn die Vorinstanz eine solche Zahlung (Honorar aus der Vermietung von D. an den Täter) nicht als ausreichend erachtet, um ein Interesse einer SDN (hier der F.) im Sinne des US-amerikanischen Cyber-Sanktionsrechts anzunehmen. Auch eine Verletzung des rechtlichen Gehörs (vgl. hiervor E. 3) ist diesbezüglich nicht ersichtlich.
Es ist nicht zu beanstanden, wenn die Vorinstanz zum Ergebnis gelangte, eine Transaktion im Zusammenhang mit einer Ransomware-Attacke (wie die Auszahlung einer Versicherungssumme) sei nur dann sanktionsrechtlich relevant, wenn mit der Transaktion ein Interesse der SDN (hier der F.) tangiert werde; wobei die Beschwerdeführerin zu weit gehe, wenn sie geltend mache, jede Nutzung von D. (auch durch Dritte) führe zu einer verbotenen Transaktion, weil F. über D. an dieser Transaktion entweder direkt oder indirekt beteiligt sei.

7.2.4. Mit den übrigen vorinstanzlichen Erwägungen (vgl. hiervor E. 7.1.2 f.) der Hauptbegründung setzt sich die Beschwerdeführerin sodann kaum auseinander, stattdessen fokussiert sie sich auf die Eventualbegründung. Sie macht hinsichtlich der erwähnten vorinstanzlichen Erwägungen der Hauptbegründung einzig noch geltend, entgegen der fehlerhaften vorinstanzlichen Auslegung (vgl. hiervor E. 6.1) spiele das Verhalten des OFAC keine Rolle. Damit genügt sie den Rügeanforderungen mangels hinreichender Auseinandersetzung mit den vorinstanzlichen Erwägungen (vgl. hiervor E. 1.1) nicht. Es ist jedenfalls nicht zu beanstanden, wenn die Vorinstanz bei der Beurteilung des Risikos einer Bestrafung der Beschwerdeführerin wegen Auszahlung der Versicherungssumme an die Beschwerdegegnerin als weiterer Faktor auch das tatsächliche Verhalten der OFAC berücksichtigt.

8.
Die Beschwerde gegen einen Entscheid, der auf mehreren selbstständigen Begründungen beruht, ist abzuweisen, sobald sich erweist, dass eine davon den dagegen vorgebrachten Rügen standhält. Damit braucht nicht auf die Rügen der Beschwerdeführerin eingegangen zu werden, die sich gegen die vorinstanzliche Schlussfolgerung richten, dass sie die von ihr behauptete Urheberschaft von F. betreffend den Programmcode von D. ohnehin nicht nachzuweisen vermöge.

9.
Nach dem Gesagten ist die Beschwerde abzuweisen, soweit darauf einzutreten ist. Bei diesem Ergebnis wird die Beschwerdeführerin kosten- und entschädigungspflichtig (Art. 66 Abs. 1 und Art. 68 Abs. 1 und 2 BGG).

Demnach erkennt das Bundesgericht:

1.
Die Beschwerde wird abgewiesen, soweit darauf einzutreten ist.

2.
Die Gerichtskosten von Fr. 12'000.-- werden der Beschwerdeführerin auferlegt.

3.
Die Beschwerdeführerin hat die Beschwerdegegnerin für das bundesgerichtliche Verfahren mit Fr. 14'000.-- zu entschädigen.

4.
Dieses Urteil wird den Parteien und dem Handelsgericht des Kantons Zürich schriftlich mitgeteilt.