CYBER INSURANCE – WHAT COVERAGE IN CASE OF AN ALLEGED ACT OF WAR?

QUESTIONS RAISED BY THE *MONDELEZ V. ZURICH* CASE

Justine Ferland[1]

ABSTRACT

In October 2018, snack company Mondelez International, Inc. (**Mondelez**) filed an action against Zurich American Insurance Company (**Zurich**), requesting indemnification for more than USD $100,000,000 in losses caused by the NotPetya cyber virus. Zurich refuses to cover these damages alleging one of the insurance policy's exclusions for damage resulting from a hostile or warlike action by a government, as the NotPetya attack is said to have been sponsored by Russia. This case is noteworthy for multiple reasons: not only is it the first significant legal dispute in the insurance field concerning the recovery of costs resulting from a cyber attack, but it is also the first time that an insurance company is invoking the war exclusion to decline coverage for an allegedly state-sponsored cyber hack.

This article analyzes the key issues of this important case, including attribution of a cyber attack to a State and interpretation of an insurance policy's war exclusion in a cyber context, and the likelihood of success of Mondelez's arguments. It also explores the strengths and limits of general principles of contract and public international law when applied to new technologies and cyber incidents. Finally, it discusses the potential impacts of the Mondelez case on the contents and limits of future traditional and cyber-specific insurance policies.

[1] Teaching and Research Assistant (University of Geneva, Switzerland) and Attorney (Quebec Bar, Canada). Contact email: Justine.Ferland@unige.ch

CYBER INSURANCE – WHAT COVERAGE IN CASE OF AN ALLEGED ACT OF WAR?

QUESTIONS RAISED BY THE *MONDELEZ V. ZURICH* CASE

1. Introduction

Over the past decade, cyber attacks have kept growing in sophistication, scope and impact, leaving businesses increasingly exposed to potential losses of significant importance. Indeed, not only may they incur direct financial costs (for instance due to theft of corporate information, business interruption or cost of repairing affected systems), but also important reputational damages – which may, in turn, lead to loss of customers, sales or profits – and legal consequences such as fines and regulatory sanctions for having compromised personal data.

Even though having a cybersecurity risk management policy and incident response plan in place is crucial and may reduce a business' risk of being exposed to and suffering from a cyber attack, it is unfortunately impossible to eliminate the risks altogether. As such, many businesses are turning towards insurance companies to ensure they have adequate protection against those risks, whether through general or cyber-specific insurance policies.

However, a recent – and still pending – U.S. case has shed light on the potential limits of insurance coverage in the context of a large-scale cyber attack. Indeed, this question is at the heart of the *Mondelez International, Inc.,* v. *Zurich American Insurance Company*[2] complaint filed in October 2018 before the state Circuit Court of Illinois.[3]

2. The facts

According to the complaint, in June 2017, Mondelez International, Inc. ("**Mondelez**"), one of the world's largest snack companies, suffered two malicious introductions of malware machine code by the NotPetya virus, which stole credentials of numerous users, propagated across the Mondelez network and rendered 1,700 servers and 24,000 laptops permanently dysfunctional. As a result, Mondelez alleges to have incurred property damage, commercial supply and distribution disruptions, unfulfilled customer orders, reduced margins, and other covered losses aggregating more than USD $100,000,000.

At the time of the attacks, Mondelez held an all-risk property insurance policy from Zurich American Insurance Company ("**Zurich**"). This insurance policy covered all risks of physical loss or damage to Mondelez's property, specifically including "physical loss or damage to electronic data, programs, or software, including physical loss or damage caused by the malicious introduction of a machine code or instruction (…)"[4]. The policy also specifically provided other types of coverage, including for "Actual Loss Sustained and extra expense incurred by the Insured during the period of interruption directly resulting from the failure of the Insured's electronic data processing equipment or media to operate"[5].

---

[2] *Mondelez Intl. Inc. v. Zurich Am. Ins. Co.*, No. 2018-L-11008, 2018 WL 4941760 (Ill. Cir. Ct., Cook Cty., complaint filed Oct. 10, 2018) (the "**Complaint**").

[3] In Illinois, the circuit court is the court of original jurisdiction. Mondelez alleges that this Court has personal jurisdiction over Zurich pursuant to article 735 ILCS 5/2-209(a)(4) of the Illinois Compiled Statutes (Complaint, par. 2). This article essentially states that any person, whether or not a citizen or resident of the State of Illinois, who contracts to insure a person, property or risk located within this State at the time of contracting, submits to the jurisdiction of the Illinois courts as to any cause of action arising from this contract.

[4] Complaint, par. 7.

[5] Complaint, par. 8.

It should be noted that this coverage was offered under a general all-risk property insurance policy and not a cyber-specific one.

Following the attacks, Mondelez requested indemnification under the Zurich insurance policy. However, Zurich refused to pay, alleging one of the policy's exclusions for damage resulting from "a hostile or warlike action" by a "government or sovereign power; military, naval or air force; or agent or authority of any [of those parties]"[6]. Indeed, the NotPetya attack is said to have originated from and been sponsored by Russia, as part of the Kremlin's ongoing effort to destabilize Ukraine (the attack had first struck in Ukraine), even though Russia vehemently denies those allegations. According to Mondelez, Zurich later rescinded its coverage denial and promised to adjust the claim, including advancement of a USD $10M partial payment. However, it never followed through; on the contrary, it raised new grounds for denying coverage in October 2018.

Mondelez therefore sued Zurich for breach of contract, alleging that Zurich's invocation of a "hostile or warlike action" to deny coverage for this incident is unprecedented and unjustified. According to Mondelez, similar exclusions have never applied to "anything other than conventional armed conflict or hostilities."[7] In addition, Mondelez alleges that this exclusion is vague and ambiguous – and hence unjustified – and thus needs to be interpreted in favor of coverage, especially since Zurich has failed to modify the historical language of the policy to specifically address the extent to which it would apply to cyber incidents.

As of today, Zurich has not yet filed its defence nor publicly commented on the lawsuit.

3. Key issues of the case

With regard to the application of insurance policy exclusions, the general rule is that the insurer – in occurrence Zurich – bears the burden of showing that a claim falls within a policy exclusion.[8] Therefore, in order to invoke the war exclusion, Zurich will have to prove that the NotPetya attack was "a hostile or warlike action" by a "government or sovereign power" or related party, which will be no easy task.

3.1 Attribution of the cyber attack to the Russian government

Whereas Ukraine, the US and UK have publicly blamed Russia for the attack[9] and the media has speculated on the subject, no official documents establishing these allegations have been published and Russia vehemently denies responsibility for the attack. It is also unlikely that national authorities could be compelled to testify or provide classified reports to support Zurich's claim since the Mondelez case is a purely private contractual matter. Zurich may therefore have difficulty proving that the

[6] Complaint, par. 13.
[7] Complaint, par. 15.
[8] *Continental Casualty Co. v. McDowell & Colantoni, Ltd.,* 668 N.E.2d 59 (1996) at 62. See also Charlotte L. WAGER and Megan A. BYRNES, "Common Exclusions and Defenses to Coverage" in *Illinois Insurance Law*, Illinois Institute for Continuing Legal Education, Springfield, 2009, p. 9-4.
[9] Notably, according to classified reports cited by U.S. intelligence officials, "the hackers worked for the military spy service's GTsST, or Main Center for Special Technology, [which] is highly involved in the GRU's [(the Russian Federation's military intelligence agency)] cyberattack program, including the enabling of influence operations." Ellen NAKASHIMA, "Russian military was behind "NotPetya" cyberattack in Ukraine, CIA concludes", *The Washington Post*, 12 January 2018, https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html?noredirect=on&utm_term=.02df391efe32 (accessed 25 February 2019). However, "the attack also hit major Russian firms, leading some cyber security researchers to suggest that Moscow was not behind it", see: "Russia behind cyber-attack, says Ukraine's security service", *BBC News*, 2 July 2017, https://www.bbc.com/news/world-europe-40471310 (accessed 25 February 2019).

NotPetya attack originates from "a government or sovereign power", thus falling within the scope of the war exclusion.

However, all hope may not be lost for Zurich since this question is raised in the context of a civil trial – based on an insurance contract – and not a criminal one. This means that Zurich will have to prove the facts supporting its defense by a preponderance of the evidence[10] (e.g. that Russia's involvement is more probable than not) and not beyond reasonable doubt as would be the case in a criminal trial. It will be interesting to see whether US courts consider that public declarations from national intelligence agencies constitute sufficient preponderant proof for Zurich to attribute the cyber attack to the Russian government.

3.2 Interpretation of the war exclusion in a cyber context

Even if Zurich is able to prove that the NotPetya attack originated from Russian authorities, it may not be sufficient to deny coverage to Mondelez. Indeed, according to the policy's wording, the attack should be a "hostile or warlike action" for the exclusion to apply. Arguably, the attack may have originated from the Russian government, the Russian military or their agents or authorities, and may have economically affected thousands of companies throughout the world, but it may not be enough to conclude that said cyber attack should be qualified as an act of war instead of a "regular" criminal act. At the heart of the *Mondelez v. Zurich* litigation therefore lies the question of whether a war exclusion worded in general terms in an all-risk property insurance policy may be interpreted to cover state-sponsored cyber attacks.[11] The Court's decision on this question will have an important impact on the development of cyber insurance law, since very few cases so far have interpreted the scope of the war exclusion in insurance policies, and none with regard to its potential application to cyber attacks.

Because such wording has been found in most insurance policies throughout the world for decades, well before the rise of cyber attacks (they have become a staple clause in insurance policies since the two World Wars)[12], it is likely that Zurich did not have cyber war in mind when drafting the contentious policy. It is therefore necessary to rely on interpretation principles to see whether this exclusion may encompass state-sponsored cyber attacks today.

In general, a court called to interpret insurance policy language must ascertain the intention of the parties. If the terms in the policy are clear and unambiguous, the court must give them their plain meaning. If they are subject to more than one reasonable interpretation within the context in which they appear, however, they are considered ambiguous and must be construed strictly against the drafter of the policy and in favor of coverage.[13] This is especially true with respect to exclusionary clauses relied on to deny coverage, which must be clear and free from doubt.[14]

---

[10] Illinois Supreme Court Committee on Pattern Jury Instructions in Civil Cases (eds.), Illinois Pattern Jury Instructions: Civil, §21.01, www.state.il.us/court/CircuitCourt/CivilJuryInstructions/21.00.pdf (accessed 1 June 2019).

[11] This could prove especially difficult since, in international law, the term "act of war" has never been defined with regard to cyberspace so far: Christopher M. SANDERS, "The Battlefield of Tomorrow, Today: Can a Cyberattack Ever Rise to an "Act of War"?", *Utah Law Review*, Vol. 2018, No. 2, Article 6, p. 503-522, at 511.

[12] Bruce D. CELEBREZZE and Elizabeth J. STEWART, "War and Peace (the Abridged Version): Application of the War and Terrorism Exclusions", *American College of Coverage and Extracontractual Counsel 5th Annual Meeting*, Chicago, 2017, p. 2.

[13] *Outboard Marine Corp. v. Liberty Mutual Insurance Co.*, 607 N.E.2d 1204 (1992) at 1217, cited in WAGER and BYRNES (n 8), p. 9-3.

[14] Id.

In the context of terrorist incidents, for instance, courts have interpreted the war exclusion narrowly, on the basis that "the purpose of an all-risk insurance contract is to protect against any insurable loss not expressly excluded by the insurer or caused by the insured" and that "a narrow reading of a contractual "act of war" exclusion thus achieves the parties' contractual intent, insulating the policyholder from loss"[15]. The characterization of a specific event as an "act of war" by public officials and/or the media, or even an official declaration of war by the government, will be taken into consideration by courts assessing evidence but does not, in itself, suffice to trigger the application of the exclusion. Rather, the Court must always refer to the intention of the parties at the time of the contract.[16]

Applying those principles to the case at issue, we may postulate that the fact that the war exclusion in Zurich's policy was not drafted with cyber attacks in mind is not an obstacle *per se* to Zurich's position, as the Court may simply interpret the policy language in light of today's situation. However, it does not clearly appear that the NotPetya cyber attack is "a hostile or warlike action" by a "government or sovereign power" – as could potentially be, for instance, the destruction of a business' premises during an armed conflict or, closer to the case at issue, damages caused by a cyber attack launched by a State with the clear intent of declaring a war. We therefore believe that a narrow interpretation of the policy's terms is required. In this case, because the insurance policy clearly included "physical loss or damage to electronic data, programs, or software, including physical loss or damage *caused by the malicious introduction of a machine code or instruction*"[17], it is reasonable to believe that Mondelez intended to be covered for the consequences of cyber attacks such as NotPetya. By interpreting the war exclusion as encompassing the damage caused by NotPetya, the Court would end up denying coverage for a specific situation that Mondelez intended – and the parties agreed – to insure; this argument strongly militates against Zurich's proposed interpretation of the policy.

4. Potentially useful legal frameworks for examining the case

The Mondelez case being a purely contractual insurance dispute between two American companies, it is unlikely that the Court will feel the need to deviate from U.S. insurance law in its judgment. However, the novel questions raised in the case could perhaps inspire the Court – or at least the parties' attorneys while developing their arguments – to look at other fields of law in order to identify some lines of thought supporting their respective positions. This section addresses two potentially useful legal frameworks to assess the case: general contract law (4.1) and public international law (4.2), and explores the arguments that could be drawn from the international "Digital Geneva Convention" project (4.3).

4.1 Under general contract law: the force majeure exemption

A force majeure clause is a common clause in contracts relieving the parties from performing their contractual obligations when certain circumstances or events beyond their control arise, rendering

[15] *In re Sept 11 Lit.*, 751 F. 3d 86, 92-93 (2d Cir. 2014). For other narrow interpretations of the scope of the war exclusion in insurance contracts, see *Pan American World Airways* v. *Aetna Casualty and Surety Co.*, 505 F. 2d 989 at 993 (2d Cir. 1974) and *Holiday Inns Inc. v. Aetna Ins. Co.*, 571 F. Supp. 1460 at 1463 (S.D.N.Y. 1983). For a general and recent recapitulation of the application of the war exclusions in the United States, see CELEBREZZE and STEWART (n 12).

[16] Christopher A. JENNINGS, "Insurance Coverage of the World Trade Center: Interpretation of "War Risk" Exclusion Clauses under the New York Contract Law" in *CRS Report for Congress,* 18 September 2011, https://www.hsdl.org/?view&did=133 (accessed 25 February 2019).

[17] Complaint, par. 7.

performance inadvisable, commercially impracticable, illegal, or impossible. Acts of war and other types of armed conflicts are frequently identified in contracts as circumstances of force majeure.[18]

The concept of force majeure can be found in most legal systems, although interpretation of its scope vary greatly.[19] The concept is generally accepted in the United States, where it is sometimes known as the doctrine of "impracticability" and "frustration of purpose".[20] Under most national laws, force majeure events must usually meet the following criteria to be considered a valid excuse for performance: "unforeseeability, unavoidability, the fact that events are outside the control of the parties and the effect of rendering performance of the obligation impossible."[21] In general, however, "clauses which contain a definition of force majeure fail to include one or another of these criteria, or express them in a less rigorous manner."[22] Since contractual dispositions generally prevail over common law, Courts must therefore look at the specific wording of a force majeure clause to interpret its scope, enforceability and effects.

The exclusion clause found in the Zurich policy is not a force majeure clause as it does not excuse performance of the insurance contract upon occurrence of certain unexpected events; it rather excludes damages caused by specific events from the scope of the contract, which otherwise remains enforceable. The principles developed under the force majeure doctrine could however still serve as inspiration as there are inevitably some similarities between the two types of clauses.

When a specific list of force majeure events is provided, courts tend to interpret force majeure clauses narrowly; that is, only the events listed and events similar to those listed will be covered. "For example, while acts of terrorism might be a specified force majeure event, it does not necessarily follow that a court would also excuse a party's performance based on "threats" of terrorism."[23] Moreover, in the absence of a specific contractual provision, courts are hesitant to characterize financial hardship due to a posterior event as a force majeure event.[24]

Applying those general principles to the case at issue, there is no doubt that cyber attacks may have potentially enormous financial consequences on businesses and thus, on their insurers. However, Zurich agreed to insure Mondelez against damages caused by the "malicious introduction of a machine code or instruction" and – although this information does not appear from the Complaint – likely confirmed the maximum liability amount that it was ready to assume via the contractual insurance limit. The fact that the NotPetya attack may be linked to Russian government agents and may have caused a greater amount of damages than what was contemplated upon the contract's conclusion, and the fact that cyber damage is currently difficult to anticipate and quantify, should not, in itself, excuse Zurich from performing its contractual obligations in the absence of clear proof establishing

[18] Marcel FONTAINE and Filip DE LY, *Drafting International Contracts*, *An Analysis of Contract Clauses*, Brill/ Nijhoff, 2009, p. 409.
[19] Id., p. 439-440.
[20] Id., p. 440; Timothy MURRAY, "Drafting Active: Avoiding Disastrous Force Majeure Clauses", *The Lexis Practice Advisor Journal,* 2 February 2018, https://www.lexisnexis.com/lexis-practice-advisor/the-journal/b/lpa/posts/drafting-advice-avoiding-disastrous-force-majeure-clauses (last accessed 28 February 2019).
[21] FONTAINE/DE LY (n 18), p. 403.
[22] Id.
[23] Janice M. RYAN, "Understanding Force Majeure Clauses", *Venable LLP*, February 2011, https://www.venable.com/insights/publications/2011/02/understanding-force-majeure-clauses (last accessed 28 February 2019).
[24] MURRAY (n 20), citing *Kyocera Corp. v. Hemlock Semiconductor LLC*, 886 N.W.2d 445 (Mich. Ct. App. 2015) as an example.

that the NotPetya attack was a "warlike action" (instead of a regular cyber attack) allowing the enforcement of the policy exception.[25]

4.2 Under public international law

According to some authors, the term "act of war" originates from international law, where it is defined as a ""use of force or other action by one state against another", which "[t]he state acted against recognizes […] as an act of war, either by use of retaliatory force or a declaration of war"".[26] In that light, public international law – and more specifically the law of armed conflict – may provide useful guidance to help interpret the insurance policy and determine whether the NotPetya attack could be qualified as an act of war.

As explained by SANDERS, the international "act of war" definition cited above requires us to analyze how a victim nation has itself defined "act of war" under its national laws. In the United States, this expression is codified as "any act occurring in the course of – (A) declared war; (B) armed conflict, whether or not war has been declared, between two or more nations; or (C) armed conflict between military forces of any origin"[27].

Because cyber attacks do not involve arms in the traditional sense, they leave a persistent confusion as to what – if anything – could constitute an act of war in cyberspace.[28] However, all the latest international developments seem to confirm that a cyber attack may, in certain circumstances, be qualified as an act of war.

Under international law, two articles of the United Nations Charter are especially relevant. Article 2(4) of this Charter states that "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in other manner inconsistent with the Purposes of the United Nations." Article 51 states that "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations […]". These articles predate the Internet era but recent doctrinal[29] and jurisprudential[30] developments support the conclusion that the use of any weapon – including a "cyber" weapon such as a computer – can constitute unlawful use of force and/or an armed attack opening the right to self-defence.

The same conclusion may be drawn when analyzing national legal systems. In the United States, for instance, the Department of Defense's 2015 *Law of War Manual*[31] is clear to the effect that international law of war principles apply to cyber operations – albeit precisely how they apply is not

---

[25] The party invoking force majeure must prove its occurrence: FONTAINE/DE LY (n 18), p. 421.
[26] SANDERS (n 11) at 511, citing Desiree GARGANO, "An Act of War: Finding A Meaning for What congress Has Left Undefined", (2012) 29 Touro L. Rev. 147 at 152.
[27] 18 U.S.C. §2331(4).
[28] SANDERS (n 11) at 511.
[29] See notably Michael N. SCHMITT (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, https://ccdcoe.org/research/tallinn-manual/ (last accessed 25 February 2019) ("**Tallinn Manual**"), Rule 14(1) and SANDERS (n 11) at 514.
[30] *Legality of the Threat or Use of Nuclear Weapons,* Advisory Opinion, 1996 I.C.J. 226 (8 July 1996) at 244.
[31] U.S. DEPARTMENT OF DEFENSE, *Law of War Manual,* June 2015 (Updated December 2016), https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190 (last accessed 25 February 2019).

yet well-settled.[32] As such, "cyberspace is an operational domain in which the armed forces must be able to defend and operate, just like the land, sea, air, and space domains."[33]

Similarly, in 2017, the European Union ministers of foreign affairs endorsed the development of a framework for a joint EU diplomatic response to malicious cyber activities – the Cyber Diplomacy Toolbox (CDT) – stating that "malicious cyber activities might constitute wrongful acts under international law", that "existing international law is applicable to cyberspace" and that "measures within the Common Foreign and Security Policy […] are suitable" in response to malicious cyber activities.[34] The framework was later expanded with a document containing implementing guidelines.[35]

The *Tallinn Manual on the International Law Applicable to Cyber Operations,* an academic, non-binding study authored by international law experts said to be the most comprehensive analysis of how international law applies to cyber conflicts[36], also concludes similarly.

Many questions regarding how international law of armed conflict principles may be transposed in cyberspace remain to be answered. However, it suffices to conclude, for the purposes of our analysis, that the actual state of law permits qualification of a State-sponsored cyber attack as an "armed attack" or "act of war" under international law of armed conflict principles in certain circumstances.

The question remains, however, regarding the threshold required for a cyber attack to constitute an "armed attack" or "act of war" (instead of a "regular" criminal act). Arguably, not every cyber attack – even when emanating from a government or State military unit – will reach this threshold.

The Tallinn Manual suggests an answer by stating that a cyber attack is an "attack" under the law of international armed conflict principles when it is "reasonably expected to cause injury or death to persons or damage or destruction to objects."[37] Indeed, "[t]he crux of the notion lies in the effects that are caused. Restated, the consequences of an operation, not its nature, are what generally determine the scope of the term 'attack'; 'violence' must be considered in the sense of violent consequences and is not limited to violent acts. For instance, a cyber operation that alters the running of a Supervisory control and data acquisition (SCADA) system controlling an electrical grid and results in a fire qualifies. Since the consequences are destructive, the operation is an attack."[38]

Under this definition, SANDERS postulates that if the 9/11 attacks had occurred through electronic hijacking rather than direct hijacking, they could still amount to an armed attack or act of war under the law of armed conflict principles[39] (provided that attribution may be properly established). The Stuxnet computer worm that infected Iranian centrifuges, causing large-scale accidents and loss of lives, and that is believed to be a jointly built American and Israeli cyberweapon, can also be seen

---

[32] Id., p. 994 ff.
[33] Id., p. 995.
[34] COUNCIL OF THE EUROPEAN UNION, *Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"),* 10474/17, 19 June 2017, http://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf (last accessed 25 February 2019).
[35] COUNCIL OF THE EUROPEAN UNION, *Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities – approval of final text,* 13007/17, 9 October 2017, http://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf (last accessed 26 April 2019).
[36] Tallinn Manual (n 29).
[37] Tallinn Manual (n 29), rule 92. See also Djemila CARRON, "L'acte déclencheur d'un conflit armé international", Ph.D. Thesis, University of Geneva, 2015, https://archive-ouverte.unige.ch/unige:75120 (last accessed 26 April 2019), p. 235 and the other references cited in CARRON's footnote 1307 at p. 235.
[38] Tallinn Manual (n 29), rule 92(3).
[39] SANDERS (n 11).

as meeting this threshold – and is, according to some experts, perhaps the only allegedly State-sponsored cyber attack to have reached it so far.[40]

Cyber attacks targeting data – as was the case with the NotPetya attack – are not *per se* excluded from this definition. The Tallinn Manual specifies that "[w]henever an attack on data foreseeably results in the injury or death of individuals or damage or destruction of physical objects, those individuals or objects constitute the 'object of attack' and the operation therefore qualifies as an attack."[41]

On the contrary, when a cyber attack destroys data and thus causes electronics to become "out of order" (without destroying the machines themselves in the traditional sense), most authors are of the opinion that the threshold to start an armed conflict is not met.[42] Similarly, if a cyber attack merely causes disruption or has non-destructive consequences (such as cyber espionage), it will likely not reach the required threshold to be seen as "use of force" under article 2(4) of the United Nations Charter, nor an "armed attack" giving rise to the right of self-defence under article 51 of the United Nations Charter.

Some authors have adopted a middle position by postulating that there may be damage or destruction of physical objects amounting to an act of war following a cyber attack "if the control system or components of it require replacement as a result. […] If repair, in the form of system or essential component replacement, is required in order to restore the functionality, then damage has been done with the consequence that the cyber event that precipitated the state of affairs can properly be described as a cyber attack"[43] amounting to an armed attack or act of war. [44]

The diverging opinions discussed above confirm that it will likely be extremely difficult to qualify the NotPetya attack under the law of international armed conflict principles. From the author's understanding of the Complaint, the NotPetya attack not only caused massive damage to data, programs and software for Mondelez, but also destroyed a substantial part of its physical equipment and components by rendering them permanently dysfunctional.[45] This could be an argument in Zurich's favour to qualify this cyber attack as an act of war.

However, the damages suffered by Mondelez could also be qualified as economic losses (rather than "property destruction" in the sense of law of armed conflict principles). The question of when, if ever, economic damages alone may be important enough to entail qualification of a cyber attack as an "attack" under the law of armed conflict has not yet been answered. Traditional law of armed conflict definitions do not consider the purely economic consequences of an event. As such, according to some experts who issued an opinion on the subject a few months before the Mondelez litigation started,

---

[40] Justin LYNCH, "Cyber ambiguity : NATO's digital defense in doubt amid unstable alliances", Defense News, 10 July 2018, https://www.defensenews.com/international/2018/07/09/cyber-ambiguity-natos-digital-defense-in-doubt-amid-unstable-alliances/

[41] Tallinn Manual (n 29), Rule 92(6).

[42] CARRON (n 37), p. 236. However, CARRON specifies that the IRCC is of a different opinion and rather holds that any cyber operation causing the deactivation of neutralisation of computer systems may amount to an armed attack under international law.

[43] William H. BOOTHBY, "Where Do Cyber Hostilities Fit in the International Law Maze?", *New Technologies and the Law of Armed Conflict,* Nasu Hitoshi and McLaughlin Robert (eds), The Hague: Asser Press, 2014, p. 59-74, at 61-62 (cited in CARRON (n 37) p. 237).

[44] CARRON (n 37), p. 237.

[45] Complaint, par. 9.

precedent suggests that the NotPetya attack may not have reached the required threshold to be qualified as a cyber "act of war" under these principles.[46]

This position is however increasingly criticized because economic damages can, in fact, "be as harmful to a nation state and result in proximate harm to the citizen's persons and property"[47] in a cyber context. The NotPetya attack is, without a doubt, one of the most onerous (in terms of economic damages) having occurred so far. It was dubbed by some journalists as being "the most devastating cyber attack in history"[48]. Although NotPetya initially appeared to be ransomware – a type of malicious software designed to block access to a computer system until a sum of money is paid – it was later established that the virus was never meant to be decrypted even if victims attempted to pay the ransom.[49] As such, it was only meant to definitely destroy data and cause chaos, an action that may arguably be equated to the "damage or destruction to objects" criteria of the Tallinn Manual, just like a bomb dropped on an empty factory in a more classic scenario. In fact, NotPetya may have caused much more economic damage to governments and civilians alike than this hypothetical bomb.

In sum, should the Court eventually consider, under the balance of probabilities, that Russia is indeed behind the attack, such attack is likely to be qualified as a criminal act but much less likely to reach the "hostile or warlike" threshold necessary for the war exclusion to apply – which requires much more than proving that a nation State acted with malicious intent.

4.3 Under a potential "Digital Geneva Convention"?

As we have demonstrated in the previous section, the applicability of general international law principles in the context of cyber conflicts poses numerous issues of applicability and interpretation that may not be easily settled and may not grant adequate protection to the collateral victims of such conflicts. As such, the scope of large-scale cyberattacks such as NotPetya shed light on the still unregulated dangers associated with the increasing implementation of technology in all aspects of human lives, and on the necessity for the international community to take action as quickly as possible.

Against this backdrop, in February 2017, Microsoft President and Chief Legal Officer Brad Smith called for the creation of a "Digital Geneva Convention" that – akin to the 1949 Fourth Geneva Convention protecting civilians in times of war – would protect civilians from state-sponsored cyber attacks by encouraging governments to commit to "avoiding cyberattacks that target the private sector or critical infrastructure or the use of hacking to steal intellectual property"[50]. Building on the voluntary norms "aimed at promoting an open, secure, stable, accessible and peaceful ICT environment" developed in 2015 by the United Nations' Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security[51], the Digital Geneva

---

[46] MARSH, "NotPetya Was Not Cyber "War"", August 2018, https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/NotPetya-Was-Not-Cyber-War-08-2018.pdf (last accessed 26 April 2019).

[47] Priyanka R. DEV, " "Use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response", 50 Tex. Int'l L. J. 381 (2015), at 390.

[48] Andy GREENBERG, "The Untold Story of NotPetya, the most Devastating Cyberattack in History", *Wired*, 22 August 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (last accessed 25 February 2019).

[49] BBC NEWS (n 9).

[50] MICROSOFT, "The need for a Digital Geneva Convention", 14 February 2017, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/ (last accessed 20 May 2019).

[51] UNITED NATIONS GENERAL ASSEMBLY, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Note by the Secretary-General", Seventieth session, Item 93 on the provisional agenda, Developments in the field of information and

Convention would go a step further and create a legally binding framework to govern states' behavior in cyberspace.[52] Through this Convention, nation States would pledge to refrain from launching cyber attacks at civilians and infrastructures in times of peace, notably by committing to (1) refrain from targeting critical infrastructures and systems whose destruction could damage the global economy or otherwise cause major global disruption, to (2) exercise restraint in developing cyber weapons and to (3) limit offensive operations to avoid creating mass damage to civilian infrastructure or facilities.[53] Companies in the tech sector have already taken important steps to limit such cyber attacks and mitigate their effects. In particular, they have recently adopted the Cybersecurity Tech Accord[54] in which businesses pledge to protect consumers worldwide and to refrain from aiding governments to carry out cyber attacks.

Although the project of a Digital Geneva Convention is still in its early stages, may never materialize due to States' very different interests in cybersecurity matters and has obviously no legal effect in the Mondelez case, it will be interesting to see how it possibly helps the development of international "cyber" law and affects the assessment of cases similar to Mondelez in the future.

5. Potential impact of the Mondelez case

This case is noteworthy for multiple reasons: not only is it the first significant legal dispute in the insurance field concerning the recovery of costs resulting from a cyber attack,[55] but it is also the first time that an insurance company is invoking the war exclusion to decline coverage for an allegedly state-sponsored cyber hack.[56] Should it proceed to trial and notwithstanding who is the successful party, it is therefore certain to have important impacts on the contents and limits of future traditional and cyber-specific insurance policies.

In the meantime, with cyber risks continually increasing and fast technological developments making it realistically impossible to predict the form, scope and consequences of the next large-scale cyber attack, both businesses and insurers should reflect on the contents and limits of their present and future insurance policies.

Given the dramatic consequences of state-attributed cyber hacks such as WannaCry, Petya and NotPetya and the likelihood of similar attacks being launched in the future,[57] insurers may increasingly try to limit potential payouts by invoking arguments similar to Zurich's. As such, businesses should ensure that their insurance policies clearly cover cyber damage allegedly caused by state actors or state representatives. They should also ensure that other exclusions generally found in insurance

---

telecommunications in the context of international security, A/70/174, 22 July 2015, https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 (last accessed 20 May 2019).

[52] MICROSOFT POLICY PAPERS, "A Digital Geneva Convention to protect cyberspace", https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH (last accessed 20 May 2019).

[53] Id.

[54] See https://cybertechaccord.org/ (last accessed 20 May 2019). To date, approximately 50 tech companies have adhered to the Tech Accord.

[55] STEPHENSON HARWOOD, "Data Protection update – January 2019", http://www.shlegal.com/insights/data-protection-update---january-2019 (last accessed 25 February 2019); Oliver RALPH and Robert ARMSTRONG, "Mondelez sues Zurich in test for cyber hack insurance", *The Financial Times,* 10 January 2019, https://www.ft.com/content/8db7251c-1411-11e9-a581-4ff78404524e (last accessed 25 February 2019).

[56] RALPH and ARMSTRONG (n 55).

[57] Jose PAGLIERY and Ryan BROWNE, "US military given more authority to launch preventative cyberattacks", *CNN Politics,* 18 September 2018, https://edition.cnn.com/2018/09/18/politics/us-military-cyberattacks-authority/index.html (last accessed 25 February 2019). PAGLIERY and BROWNE explain that US military has recently been granted more authority to launch preventative cyberstrikes against foreign government hackers, which could have collateral consequences just like the NotPetya hack allegedly did.

policies, such as exclusions for intentional or insider acts, do not limit the cyber coverage they are seeking.

In addition, businesses relying on their all-risk property insurance policy (or other traditional insurance policies) to cover the consequences of potential cyber attacks may wish to seek additional specific cyber insurance coverage to avoid ending up in Mondelez's situation, even when their general policies seem to be applicable in cases of "malicious introduction of a machine code or instruction". Indeed, according to cyber insurance specialists, this kind of "silent cyber exposure" – e.g. cyber exposures contained within traditional property and liability insurance policies that do not implicitly include or exclude cyber risks – is currently one of the insurance industry's biggest worries about cyber attacks.[58] Because a large portion of the (huge and unanticipated) recent cyberattacks impacts on insurers have been based on general insurance policies that were not explicitly designed to cover cyber attacks in the first place, insurers are now looking to protect themselves against these types of cyber loss events[59] and Zurich may be testing the courts on this point.[60] In the author's opinion, however, the Mondelez case may not be the ideal forum to test the limits of silent cyber exposure since the Policy clearly provided coverage for "malicious introduction of a machine code or instruction" – a provision that can hardly be construed as meaning anything but a cyber attack.[61] Nevertheless, as the market for cyber-specific insurance policies is already booming – according to a recent PWC study, "annual gross written premiums [for cyber insurance] are set to grow from around $2.5 billion today to reach $7.5 billion by the end of the decade"[62] – and cyber-specific insurance policies are being increasingly tailored to businesses' specific needs[63], it will be interesting to see how the *Mondelez v. Zurich* case further influences the industry.

As for insurance companies, if they wish to keep a general war exclusion in their traditional and cyber policies, they should ensure that the wording of the exclusion leaves no ambiguity concerning the circumstances in which it may apply. In addition, previous events of unforeseen scope and consequences, such as the terrorist attacks of 9/11, have already forced insurers to re-evaluate the

[58] RALPH and ARMSTRONG (n 55). Both the UK Prudential Regulatory Authority (PRA) and the European Insurance and Occupational Pension Authority have also referred to silent cyber exposure as a key concern and call on insurers to "make more progress in improving their ability to identify, quantify and manage cyber risk": Andrew MILNE, Tristan HALL and Amit TYAGI, "Drawing the line under silent cyber", CMS, 17 May 2019, available online: http://www.cms-lawnow.com/ealerts/2019/05/drawing-the-line-under-silent-cyber?cc_lang=en (last accessed 20 May 2019).

[59] According to Property Claim Services (PCS) the total industry loss from the Petya/NotPetya cyber attack is now over USD $3 billion, roughly 90% of which is the result of silent cyber exposure. See Steve EVANS, "Petya cyber industry loss passes $3bn driven by Merck & silent cyber: PCS" in *Reinsurance News,* 7 November 2018, https://www.reinsurancene.ws/petya-cyber-industry-loss-passes-3bn-driven-by-merck-silent-cyber-pcs/ (last accessed 25 February 2019).

[60] RALPH and ARMSTRONG (n 55).

[61] In a 2017 report, the Organization for Economic Co-operation and Development (OECD) reminded that "[c]overage may be provided as a stand-alone policy, *as a specific endorsement on existing policies (e.g., where coverage for specific losses is added to a property policy)* or as part of traditional coverages without a specific endorsement (often referred to as silent cyber coverage) [italics added by author]" and that "[g]iven that cyber risks are not consistently excluded from traditional policies, the purchase of specific cyberinsurance coverage by all companies should not be necessary." OECD, "Supporting an Effective Cyber Insurance Market", *OECD Report for the G7 Presidency*, May 2017, pp. 5 and 7, http://www.oecd.org/daf/fin/insurance/Supporting-an-effective-cyber-insurance-market.pdf (last accessed 26 April 2019).

[62] PWC, "Insurance 2020 & beyond: Reaping the dividends of cyber resilience", 2015, https://www.pwc.com/gx/en/industries/financial-services/publications/insurance-2020-cyber.html (last accessed 26 April 2019).

[63] For instance, many insurance companies in Switzerland and abroad are now offering cyber insurance for SMEs.

efficacy and scope of their standard war risk exclusions, as well as their underwriting practices and reserves.[64] There is no doubt that today's sophisticated and continually evolving cyber crime methods need to be taken into account in a similar fashion. Should Mondelez win this case, insurers will need to thoroughly review the wording of their policies to clearly circumscribe the scope of their obligations in case of large-scale cyber attacks. In addition, should they wish to offer coverage in those situations, they will need to ensure to remain in sufficiently good financial health to cover the potentially enormous (and difficult to assess in advance) damages caused by these attacks.

Furthermore, because uncertainty about exposure is one of the main factors impending the availability and affordability of cyber insurance coverage and reducing companies' willingness to pay for that coverage[65], all insurance companies should also aim to work together in improving the data available for quantifying exposure[66] – something that may be facilitated by national governments and international organizations such as the OECD and WEF. Insurance companies could also incentivise cybersecurity risk mitigation by offering cheaper insurance to their clients contingent on better cybersecurity measures.[67]

Finally, all businesses – including insurance companies themselves, who are not exempt from being targeted in a future cyber attack! – should keep in mind that strong cybersecurity measures and a comprehensive cyber risk management policy are always the best defence to potentially wrecking cyber attacks, notwithstanding their author and the motives behind them.

[64] Jeffrey W. STEMPEL, "The Insurance Aftermath of September 11: Myriad Claims, Multiple Lines, Arguments over Occurrence Counting, War Risk Exclusions, the Future of Terrorism Coverage, and New Issues of Government Role", (2002) 37 Tort & Ins. L.J. 817.
[65] OECD (n 61), pp. 11-12.
[66] Insurance experts notably came to this conclusion in a 2018 OECD Conference; OECD, "Unleashing the Potential of the Cyber Insurance Market", *Conference Outcomes*, 22-23 February 2018, Paris, France, available at http://www.oecd.org/daf/fin/insurance/Unleashing-Potential-Cyber-Insurance-Market-Summary.pdf (last accessed 26 April 2019).
[67] The World Economic Forum encourages policymakers to consider this measure: WEF, *Cyberinsurance*, available at http://reports.weforum.org/cyber-resilience/cyberinsurance/ (last accessed 26 April 2019).

ACKNOWLEDGEMENTS

This article was written in the course of a research project conducted at the Faculty of Law of the University of Geneva on cybersecurity liability (www.cybersecurity-liability.ch), in the context of a joint research project between the University of Geneva and the Hebrew University of Jerusalem. An early version of this paper was presented at the Geneva Cybersecurity Law & Policy Conference, University of Geneva (June 20, 2019).

The author would like to thank Prof. Jacques de Werra, Professor of contract law and intellectual property law at the Law School of the University of Geneva, Switzerland, for comments and input that greatly improved this article.