International
Comparative
Legal Guides

Insurance & Reinsurance 2020

A practical cross-border insight into insurance and reinsurance law

Ninth Edition

Featuring contributions from:

Advokatfirman Vinge KB
Arthur Cox
BLACK SEA LAW COMPANY
Blaney McMurtry LLP
BSA Ahmad Bin Hezeem & Associates LLP
CIS Risk Consultant Company (insurance brokers) LLP (CIS)
Clyde & Co (Deutschland) LLP
Clyde & Co LLP
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
DAC Beachcroft Colombia Abogados SAS
DAC Beachcroft LLP
DeHeng Law Offices
ENSafrica
ESENYEL & PARTNERS LAWYERS AND CONSULTANTS
ESTUDIO ARCA & PAOLI, Abogados S.A.C.
Eversheds Sutherland Ltd.
Gross Orad Schlimoff & Co.
Ince
Jurinflot International Law Firm
Kennedys
KPMG Abogados, S.L.P.
Kramer Levin Naftalis & Frankel LLP
Kvale
KYRIAKIDES GEORGOPOULOS Law Firm
Lee and Li, Attorneys-At-Law
Lee & Ko
Legance – Avvocati Associati
Lloyd's Market Association
Marval O'Farrell Mairal
Matheson
McMillan LLP
Mori Hamada & Matsumoto
NautaDutilh Avocats Luxembourg
Norton Rose Fulbright
Paul, Weiss, Rifkind, Wharton & Garrison LLP
Poul Schmith
Pramuanchai Law Office Co., Ltd.
Railas Attorneys Ltd.
Steptoe & Johnson LLP
Tavares Advogados
Tuli & Co
Vavrovsky Heine Marth Rechtsanwälte GmbH

INSIGHT CONSENSUS INFLUENCE
ICLG.com

Cyber Warfare and the Act of War Exclusion

Blaney McMurtry LLP

Dominic T. Clarke

Introduction

A recent cybersecurity breach of the Canadian laboratory testing company LifeLabs has underscored the rising threat of cyber-attacks and the significant losses attributable to them. On December 17, 2019, Canada's largest private provider of diagnostic testing for health care disclosed that it had suffered a cyber-attack that may have compromised the personal information of some 15 million customers, primarily in the provinces of British Columbia and Ontario.[1] The company is facing a putative class action lawsuit claiming for more than $1.13 billion in compensation for Lifelabs' clients, who they say experienced repercussions, including damage to their credit reputation, wasted time, inconvenience and mental distress.[2]

This was, of course, far from the first cyber-attack on a Canadian company. According to the Canadian Centre for Cyber Security, 71 per cent of Canadian organisations reported experiencing at least one cyber-attack last year, with the average cost of investigating and remediating the attack averaging at $9.25 million.[3] To protect against this kind of significant financial risk, many businesses have turned to cyber insurance.

The cyber insurance market remains relatively new and misunderstood in comparison to other lines of business. However, there is a growing acceptance by businesses across Canada of cyber insurance as an effective risk transfer solution.[4] However, the application of one common, but rarely used, provision in insurance policies has been a topic of debate in the cyber insurance context. That is the war exclusion and whether a cyber-attack could be considered an act of war.

Although the attack on LifeLabs can be characterised as an act of cyber-crime as opposed to cyber-war, renewed turmoil in the Middle East has again made the threat of war a possibility and has given the war exclusion renewed importance to the insurance industry in an age of digital warfare. This issue came to light most prominently in 2018 when one of the world's largest confectionery, food and beverage companies, Mondelez International ("Mondelez"), sued its insurer Zurich American Insurance Company ("Zurich") for denying coverage to Mondelez following the NotPetya global cyber-attacks that caused billions of dollars in damage around the world.

NotPetya Cyber-Attacks

On June 27, 2017, a major global cyber-attack began utilising a variation of Petya malware. On that day, Kaspersky Lab reported attacks in France, Germany, Italy, Poland, the United Kingdom, and the United States, as well as Russia and Ukraine, where more than 80 companies were initially attacked, including the National Bank of Ukraine. It was dubbed the "NotPetya" virus.[5]

The NotPetya virus was part of a series of attacks making use of hacking tools that were stolen from the National Security Agency of the United States. This hacking took control of computers and initially demanded ransom from their owners to regain access. It wreaked havoc around the world and was an assault that was intended to coincide with the Ukrainian public holiday of Constitution Day, hitting just on its eve.[6]

While Ukraine's government and businesses may have been the primary target, the cyber-attacks affected the computer systems of private companies throughout the world. In the United States, a multinational law firm reported being hit, while computers in a Cadbury chocolate factory in Hobart, Tasmania, owned by Mondelez, displayed ransomware messages that demanded USD $300 in bitcoins.[7] By the time the attacks were over, multiple multinational companies were severely impacted, including Maersk, pharmaceutical giant Merck, FedEx's European subsidiary TNT Express, French construction company Saint-Gobain, food producer Mondelez, and manufacturer Reckitt Benckiser.[8]

This was not, however, the work of regular criminal hackers. The CIA believed the attacks to have been a Russian state-sponsored attack on Ukraine. It concluded with a high degree of confidence that the Russian GRU military spy agency created NotPetya with the goal of disrupting Ukraine's financial system. The military hackers used malware that appeared to be ransomware, which encrypts data and decrypts it only if a ransom is paid, to make it appear as though criminal hackers were responsible rather than a nation state. Because of this deception, it took days to understand that NotPetya was permanently deleting data.[9]

The result was more than $10 billion in damage, according to Tom Bossert, a United States Homeland Security adviser at the time of the attacks. While there was no loss of life, Bossert characterised the attacks as being "the equivalent of using a nuclear bomb to achieve a small tactical victory".[10] Other reported approximate damages to specific companies included USD $870 million to Merck, USD $400 million to FedEx, USD $384 million to Saint-Gobain, USD $300 million to Maersk, and USD $188 million to Mondelez.[11] If there was ever a hacking event that could be characterised as an act of cyberwarfare on a global scale, the NotPetya virus arguably was it.

Mondelez v Zurich

Mondelez, one of the world's largest snack companies, was one of the major victims of the NotPetya cyber-attacks. The malware spread throughout its servers, stole credentials of numerous users, propagated across the Mondelez network and rendered approximately 1,700 servers and 24,000 laptops permanently dysfunctional. As a result of this damage caused to both its hardware and software systems, Mondelez alleged that it

© Published and reproduced with kind permission by Global Legal Group Ltd, London

incurred property damage, commercial supply and distribution disruptions, unfulfilled customer orders, reduced margins, and other losses well in excess of USD $100 million.[12]

Zurich provided property insurance to Mondelez at the time of the cyber-attacks. According to Mondelez's complaint against Zurich,[13] Zurich's insurance policy provided coverage at the date of loss for "all risks of physical loss or damage" to Mondelez property, including instances of "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".

The policy also provided other types of coverage including, but not limited to, time element 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" resulting from malicious cyber damage.[14] This coverage was offered under a general all-risk property insurance policy and not a cyber-specific one.

Following the cyber-attack, Mondelez alleged that it gave prompt notice to Zurich and worked with Zurich to adjust the insurance claim. However, on June 1, 2018, Zurich informed Mondelez that it was denying coverage under the Policy based on a single policy exclusion for hostile or warlike action, which provided the following:[15]

> "This Policy excludes loss or damage directly or indirectly caused by or resulting from any of the following regardless of any other cause or event, whether or not insured under this Policy, contributing concurrently or in any other sequence to the loss:
>
> 2) (a) hostile or warlike action in time of peace or war, including action in hindering, combating or defending against an actual, impending or expected attack by any: (i) government or sovereign power (de jure or de facto); (ii) military, naval, or air force; or (iii) agent or authority of any party specified in I or ii above."

According to Mondelez, Zurich relied on no other ground for denying coverage under the general all-risk property insurance policy other than the act of war exclusion. It claimed that Zurich then later rescinded its coverage denial on July 18, 2018 and promised to adjust the claim, even committing to advance a USD $10 million partial payment towards Mondelez. However, on October 9, 2018, Zurich allegedly reasserted its June declination of coverage based on the act of war exclusion.[16]

Mondelez therefore promptly sued Zurich for breach of contract.[17] Mondelez asserted that the invocation of the act of war exclusion to deny coverage for the NotPetya virus was unfounded and unprecedented and that such a clause has never applied to anything other than conventional armed conflict or hostilities. Further, Mondelez also asserted that the cyber-attack losses did not result from a cause or event excluded under the act of war exclusion and that the attack did not constitute a "hostile or warlike action" as required by it. Additionally, it argued that the exclusion itself was vague and ambiguous, particularly given Zurich's failure to modify the historical language to specifically address the extent to which it would apply to cyber incidents. Because of that, it claims that the exclusion must be interpreted in favour of coverage.[18]

As of today, Mondelez's litigation remains ongoing. After a series of motions, Zurich filed its reply in October 2019 and a continued case management date is currently set for March 2020.

Act of war exclusions such as the one invoked by Zurich, of course, have been common clauses in insurance policies for decades. However, the Mondelez case is the first time that an insurance company has invoked the exclusion to decline coverage for a cyber-attack.

The Act of War Exclusion

For the better part of a century, many insurance policies have contained terms that exclude from coverage "war risks", being losses of property or life due to acts of actual warfare. There are two important considerations on the part of insurance companies that necessitate such exclusions: the inability of insurance companies to properly gauge premiums to cover those risks; and the companies' need to protect against financial disaster which could result from wholesale death or destruction occurring from actual warfare. The rationale behind these exclusions is that if private insurers were to assume the normal risks accompanying military service in a time of war under ordinary premium rates, they could become insolvent. Instead of penalising the country by causing the bankruptcy of such insurance corporations, the courts choose to penalise the individual insureds.[19]

Courts in the United States have frequently been called on to define "acts of war" over the past century. In *Vanderbilt v. Travelers' Insurance Company*, one of the earlier cases to interpret the war exclusion and a traditional example of the clause's usage, the insured was traveling as a passenger and was on board the British steamer Lusitania, then bound from New York to Liverpool on May 7, 1915 with a life insurance policy in effect. The Lusitania was engaged as a passenger and freight ship, carrying both merchantman and non-combatants alike, when it was sunk off the coast of Ireland by a German submarine. The sinking resulted in the unfortunate death of the insured and was done at a time when a formal state of war existed and was being waged between Great Britain and Germany. However, the insured's life insurance policy contained an exclusion clause stating that the insurance would not cover death resulting from war or riot. Even though the United States was not involved in World War I at the time, the Court found that a formal war was certainly in existence and the torpedoing of a ship was considered an act of war. It further determined that the ship was sunk in accordance with the instructions of a sovereign government and came about in a contest conducted by armed public forces in a state of war. As such, a New York court held that the death of the insured was not covered by the policy excluding acts of war.[20]

In a similar case dealing with an exclusion interpreted under more traditional physical warfare, *Stankus v. New York Life Insurance Co.,* the insured was a manager on the S.S. Altalena, a vessel which was transporting munitions to Israel during an armistice between Israel and neighbouring states and which contained members of a military organisation, the Irgun, at odds with the Israeli government. On June 22, 1948, the insured was killed during an attack by artillery and machine-gun fire in the harbour of Tel Aviv by the Israeli army. Under those circumstances, the insurer invoked the act of war exclusion. Despite the armistice in place, the Court viewed this activity as an act of war by Israel and held the insured's death to be within the contemplation of a clause exempting the company from liability for death "directly or indirectly from a state of war".[21] On this basis, it was established that acts of war can take place for the purpose of insurance coverage even if a "state of war" may not currently exist.

In cases arising out of the Pearl Harbor attack, courts more comprehensively considered the distinction between acts of war and states of war. In *Gladys Ching Pang v. Sun Life Assurance Co. of Canada*, the insured, an employee of the Honolulu Fire Department, died as a result of the Japanese attack on Oahu on December 7, 1941. The insured's life insurance policy carried a double-indemnity clause, giving double the face of the policy for death caused solely by external, violent, and accidental means, but this clause expressly excluded death resulting from

© Published and reproduced with kind permission by Global Legal Group Ltd, London

riot, insurrection, or war, or any act incident thereto. While the insurer maintained that on the date of loss the United States was at war with Japan, the plaintiff beneficiary argued that there must be some recognition of the existence of war by the government before courts can take judicial notice of its existence, which the plaintiff argued only happened the next day when the United States congress passed a resolution declaring war on Japan. The Hawaii court found that "war" does not exist merely because of an armed attack by the military forces of another nation. It was held that it needed to be a condition recognised or accepted by the political authority of the government which is attacked, either through an actual declaration of war or other acts which recognise the existence of a state of war. As such, the insured's death was found to have not resulted from an act of war and coverage was granted.[22]

However, in a leading case of United States Court of Appeals, *New York Life Insurance Company v. Bennion*, the Court held that a state of war existed at the time of the Pearl Harbor bombing even though war had not yet been declared. In this case, the insured was the captain of a battleship and was killed in the attack at Pearl Harbor. The Court found nothing in the subject matter, the context, or the purpose of the insurance policy to indicate that the parties intended to use the word "war" in the technical sense of a formally declared war. The parties did not specify any particular type or kind of war, rather they used the all-inclusive term, and the Court thought it fair to assume that they had in mind any type or kind of war in which the hazard of human life was involved.[23] This decision opened the door for coverage denials involving many types of physical conflicts between countries in which war was never formally declared.

Through such American case law, two categories of war exclusion clauses arose over time: result clauses and status clauses. Typical result clauses generally excluded the insurance company from coverage obligations when the insured's death resulted from military activity in a time of war. Status clauses generally excluded the insurance company from liability from all causes while the insured was in military service in a time of war. Accordingly, in result clause cases, courts decided whether the death of the insured was the result of military activity. Status clause cases usually involved two issues, whether the insured was actually in military service and whether the death indeed happened in wartime.[24]

As more exclusion clauses exempted the insurer from liability only for death from acts of war rather than from any kind of engagement in military service, the issue before courts has routinely become whether the loss resulted from "war" itself. In these early cases on the interpretation of the term "war", courts sometimes construed the term in its legal, technical sense, requiring a "state" of war (i.e., a formally declared war), while at other times courts recognised "acts" of war (i.e., warlike hostilities) as sufficient to exclude the insurer from liability. Because of lessons learned involving the question of whether the Korean War was legally a war involving the United States, many insurance companies in their exclusion clauses now refer to a war "whether declared or undeclared".[25] In the aforementioned Mondelez case, the Zurich policy followed this approach, with its exclusion applying to warlike actions in both "a time of peace or war".

Courts have also since recognised that the interpretation of insurance policies does not turn on how political leaders describe the events giving rise to a loss, but on how the policy describes the event. If the terms in the policy are clear and unambiguous, the Court will give them their plain and ordinary meaning. Conversely, if they are considered ambiguous, as Mondelez is claiming in its suit, the rule of *contra proferentem* may apply in favour of coverage.[26]

One of the most recent cases in this area that reaffirmed the special meaning of "war" in the insurance context is *Universal Cable Productions, LLC v. Atlantic Specialty Insurance Company*[27] ("Universal"). In Universal, the insured submitted a claim for loss related to the need to relocate the production of a television series due to rocket attacks conducted by Hamas, which is affiliated with the Palestinian Authority, located in the Gaza Strip adjacent to Israel. The insured carried its burden to show that "war" had special meaning in the insurance industry that required hostilities between *de jure* and *de facto* governments. Based on the customary usage in the insurance industry of the terms "war", and "warlike action by a military force", the United States Court of Appeals, Ninth Circuit, held that the meaning of such terms related to the existence of hostilities between *de jure* or *de facto* governments. Hamas was not *de jure* or a *de facto* sovereign, and therefore actions by that organisation could not be defined as "war" for purposes of interpreting war exclusion. As such, the "war" and "warlike actions" exclusions in policy were not triggered.[28]

Cyber Warfare: A Changing Coverage Landscape

With regard to the application of insurance policy exclusions, the general rule is that the insurer bears the burden of showing that a claim falls within a policy exclusion. Therefore, in order to invoke the war exclusion in the cyber context, insurers such as Zurich have the difficult task of proving that a cyber-attack was a warlike action by a government or sovereign power (or by an agent or authority of such a power) rather than a criminal or terrorist action.

It has been challenging for insurers to establish that "regular" hostilities had significant attributes of sovereignty in the past. For example, in the seminal case *Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co*, despite arguments from the insurer that the Popular Front for the Liberation of Palestine (PFLP) was a quasi-government body that received financial support and arms from China and North Korea, a court held that its hijacking of a plane in 1970 was the act of a radical political group rather than a sovereign government and that the loss of the plane was in no sense caused by any "war" being waged by or between recognised states. The PFLP had not been accorded by Middle Eastern states the rights of a government, nor could the PFLP's own exaggerated rhetoric, proclaiming itself to be "at war with the entire Western World", change the practical realities that the hijackers were not the agents of a sovereign government.[29] In subsequent cases, courts have generally followed the *Pan Am* court's reasoning when deciding whether war exclusions apply to acts of terrorism.[30]

In the context of cyber-attacks from groups with unofficial links to a state and whose origin can be disguised by the professional hackers who commit them, establishing the sovereign nature of such actions will become even more difficult. While the aforementioned Mondelez cyber-attack was widely believed to have been a Russian state-sponsored attack, Russia denied responsibility for the attack.[31] For the policy exclusion to apply to cyber-warfare, insurers such as Zurich will have to establish sufficient evidence of a connection between cyber-attacks and a government or sovereign power. Without official documentation in support and given the shrouded nature of cyber-attacks and the motives behind them, that will probably not prove easy for insurers.

Beyond the issue of attribution, insurers will also have to show that any cyber-attack constitutes a "warlike action" rather than a traditional criminal or terrorist action for the policy exclusion to apply. One obstacle facing insurers in this regard is that a court must determine what the intent of the parties was at the time of

© Published and reproduced with kind permission by Global Legal Group Ltd, London

the contract and, as noted, that any ambiguity in a policy exclusion is generally construed against the insurer and in favour of the insured.[32] Courts need to construe the exclusions as parties would reasonably have expected them to be construed.[33] As the wording of these war clauses has been found in most insurance policies for nearly a century, long before cyber-attacks become a mode of conflict, cyber warfare is likely not something that would have been anticipated by either party as being a "warlike action" under an insurance policy.

In this regard, a leading insurance treatise notes that "warlike operations" are normally part of an armed conflict between combatants and usually do not include intentional violence against civilians by political groups.[34] Past coverage case law has also distinguished between warlike operations and terrorist activity, with courts historically viewing "warlike operations" as not including attacks upon civilian citizens of non-belligerent powers and their property.[35]

Cyber-attacks, however, regularly involve attempts to alter, disable, steal, and destroy property of civilians and private corporations such as Mondelez. While such attacks target computer systems, networks, and infrastructures that can cause millions of dollars in losses, they do not easily fall into the traditional definition of "warlike operations". To have a chance at success, insurers such as Zurich will have to contend that the nature of warfare has changed, that attacks on the private sector are a tactic now used in modern global warfare, and consequently that courts reading clauses such as "war" and "warlike operation" as narrowly as in the past is no longer appropriate.

This will be likely be problematic for insurers given that war exclusions were developed with physical conflicts between states in mind. They were originally designed and applied to limit insurer risk for loss and damage sustained physically by individuals during a formal state of war. They were certainly not intended to be invoked in cases of pure economic loss by third-party corporations. But given that cyber-attacks have suddenly become a legitimate tactic between governments in modern warfare, there is certainly a possibility that such exclusion clauses could begin to be interpreted much more broadly.

A potential argument in insurers' favour might be that cyber warfare is already causing nations to strike back with traditional physical combat. On May 5, 2019, the Israel Defence Forces reported that it stopped an attempted cyberattack by Hamas and retaliated with an airstrike against the building from where it said the attack originated.[36] While this direct meeting of a cyber-attack with a real-world response during an ongoing battle may have been a potential first for cyberwarfare, physical retaliation of this kind will no doubt become more common. As cyber-attacks get more severe and hackers inflict real-world harm through critical infrastructure hacking, escalating physical warfare in response by government and sovereign powers appears inevitable.

In determining the Mondelez case and future cyber warfare coverage cases that will likely follow it, courts will have to decide whether the consequences of such cyber-attacks need to go beyond economic losses to the point of casualties or wreckage seen in previous interpretations of the war exclusion for the act of war exclusion to apply. As war evolves in the digital age, however, it is reasonable to anticipate that the interpretation of the war exclusion will evolve with it.

Conclusion

With more and more nations developing advanced cyber warfare operations to weaken enemies and strengthen their own global positions, cyber-attacks such as the NotPetya virus will only become more frequent in number and wide in scope. Cyber warfare may even be the way that future conflicts between nation states are both predominantly fought and won. As that happens, cases such as *Mondelez v. Zurich* will become all the more common.

Given these developments in modern warfare, it would be wise for insurers to reconsider their all-risk property and cyber insurance policies and clearly define what the exclusions and limits of those policies are. For now, although change may be on the horizon, this issue has not yet been judicially analysed and is far from being conclusively resolved.

Acknowledgment

The author would like to acknowledge and thank Blaney McMurtry Associate Stephen Gray for his contributions to the substance of this chapter.

Endnotes

1. Charles Brown, Life Labs Customer Notice (updated January 2020), online: LifeLabs https://customernotice.lifelabs.com/.
2. Cole Burston, *LifeLabs facing proposed class action lawsuit over data breach* (December 2019), online: The Globe and Mail https://www.theglobeandmail.com/business/article-life-labs-facing-proposed-class-action-lawsuit-over-data-breach/.
3. 2019 CIRA Cybersecurity Survey, online: CIRA https://cira.ca/resources/cybersecurityreport/2019-cira-cybersecurity -survey.
4. Paul Kovacs, *Cyber Risks 2019: Implications for the insurance industry in Canada* (July 2019), The Insurance Institute of Canada.
5. *Global ransomware attack causes chaos* (June 2017), online: BBC News https://www.bbc.com/news/technology-40416611.
6. Nicole Perlroth, Mark Scott, and Sheera Frenkel, *Cyberattack hits Ukraine then spreads internationally* (June 2017), online: *The New York Times* https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html.
7. *Ibid.*
8. Andy Greenberg, *The untold story of NotPetya, the most devastating cyberattack in history* (August 2018), online: *Wired* https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
9. Ellen Nakashima, *Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes* (January 2018), online: *The Washington Post* https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes.
10. *Greenberg*, *supra* note 8.
11. *Greenberg*, *supra* note 8.
12. *Mondelez Intl. Inc. v. Zurich Am. Ins. Co.*, No. 2018-L-11008, 2018 WL 4941760 (Ill. Cir. Ct., Cook Cty., complaint filed October 10, 2018) (the "Complaint").
13. *Complaint*, *supra* note 12 at para. 7.
14. *Complaint*, *supra* note 12 at para. 8.
15. *Complaint*, *supra* note 12 at para. 13.
16. *Complaint*, *supra* note 12 at paras 13–22.
17. Justine Ferland, "Cyber insurance – What coverage in case of an alleged act of War? Questions raised by the Mondelez v. Zurich case", *Computer Law & Society Review* 35 (2019) 369–376.
18. *Complaint*, paras 13–22.
19. Sidney I. Simon, "The Dilemma of War and Military Exclusion Clauses in Insurance Contracts" (1981) 19:1 ABLJ 31 at 31; *Shneiderman v. Metropolitan Cas. Co. of N.Y.*, 220 N.Y.S.2d 947 (1961) at para. 13.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

20. *Vanderbilt v. Travelers' Ins. Co.*, 112 Misc. 248, 184 N.Y.S. 54 (1920), *affd,* 194 N.Y.S.986.
21. *Stawski v. John Hancock Mut. Life Ins. Co.*, 163 N.Y.S.2d 155 (1957).
22. *Gladys Ching Pang v. Sun Life Assurance Co. of Canada*, 37 Haw. 288 (1945).
23. *New York Life Insurance v. Bennion*, 158 F.2d 260 (10th Cir. 1946).
24. *Simon*, *supra* note 19 at 35.
25. *Simon*, *supra* note 19 at 43.
26. *Universal Cable Productions, LLC v. Atlantic Specialty Insurance Company.* 929 F.3d 1143, 9th Cir. (Cal 2019).
27. *Ibid.*
28. *Ibid.*
29. *Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co.*, 505 F.2d 989 (USCA 1974).
30. Bill Boeck, *War Exclusions and Cyber Attacks* (February 2019), online: *The D&O Diary* https://www.dandodiary.com/2019/02/articles/cyber-liability/guest-post-war-exclusions-cyber-attacks/.
31. Ivana Kottasova, *U.K. blames Russia for crippling cyberattack* (February 2018), online: CNN https://money.cnn.com/2018/02/15/technology/russia-cyberattack-notpetya-uk/index.html.
32. *Universal*, *supra* note 15.
33. *Pan Am*, *supra* note 16 at 9.
34. Steven Plitt, Daniel Maldonado, Joshua D. Rogers, and Jordan R. Plitt, *Couch on Insurance* (3rd edition, 2017) at § 152:3–4.
35. *Pan Am*, *supra* note 16 at 17.
36. Lily Hay Newman, *What Israel's Strike on Hamas Hackers Means for Cyberwar* (May 2019), online: *Wired* https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Dominic T. Clarke practises principally in the area of insurance litigation encompassing both coverage and defence matters. A "go-to" counsel for insurers both nationally and internationally, Dominic's expertise is sought out on large and complex coverage claims. He specialises in advising and representing insurers with respect to commercial general liability, directors' and officers' liability and commercial property policies. He has significant experience in the defence of products liability and sexual abuse litigation. A force in the courtroom, he has appeared in the Ontario Superior Court of Justice and the Ontario Court of Appeal. A leading expert in insurance coverage and reinsurance matters, Dominic is a frequent lecturer and is hailed as "very experienced, very agreeable and highly competent" by *Who's Who Legal*, with respondents drawing praise for his litigation practice, especially in coverage disputes. He has published numerous thought leadership pieces in his nearly three decades of practice.

Blaney McMurtry LLP
2 Queen Street East, Suite 1500
Toronto
Canada

Tel: +1 416 593 3968
Email: dclarke@blaney.com
URL: www.blaney.com

Blaney McMurtry LLP is a prominent, Toronto-based law firm consistently ranked as a top-tier regional firm, delivering top-level expertise in litigation & advocacy, real estate and business law.

Recognised as a leader in providing services to the insurance industry, in both coverage and defence work, many of the firm's insurance clients have worked with them for more than 20 years.

The firm's location in Canada's financial centre positions Blaney McMurtry to handle complex matters that have scope beyond Toronto and the surrounding area. Canadian experience delivered from one office.

Blaney McMurtry is a founding member of Insurance Law Global (ILG), a network of like-minded, independent insurance defence firms committed to providing global service to insurance clients from independent law firms across Europe and North America. In addition, the firm is also a member of the Risk Management Counsel of Canada, a national association of law firms providing services to the risk management industry; and of TAGLaw®, a worldwide network of independent law firms, ranked by *Chambers & Partners* as an "Elite" legal alliance.

www.blaney.com

© Published and reproduced with kind permission by Global Legal Group Ltd, London