NotPetya: A Particularly GRU-some Cyber Attack

Philip C. Silverberg and Hilary M. Henkind
Mound Cotton Wollan & Greengrass LLP

I. THE NOTPETYA CYBER ATTACK

On June 27, 2017, on the eve of Ukraine's Constitution Day, companies doing business in Ukraine were stunned when a message popped up on their computer screens advising that the user's "imported files are encrypted." Disguised as ransomware, the cyber attack, dubbed NotPetya, intentionally damaged critical infrastructure, by wiping data at 22 banks, four hospitals, six power companies, two airports, ATMs and card payment systems in retailers and transport, and practically every federal agency in Ukraine. Although the NotPetya attack targeted Ukraine, the nature of the attack led to indiscriminate, widespread, significant damage, not only to computers and servers of Ukrainian government offices and institutions focused on the public good (such as hospitals), but also to multinational companies doing business in Ukraine, including Merck, Mondelez, and Maersk, to name a few.

The NotPetya malware was introduced into computer networks by means of a "backdoor" in a Ukrainian tax software package called M.E. Doc. As the first step in the NotPetya attack, a malicious actor secretly compromised the company Intellect Service, the developer of M.E. Doc., by inserting malicious computer code into the legitimate M.E. Doc software, adding a backdoor that functioned as a remote access tool or "RAT." Once installed, the compromised M.E. Doc software with the RAT functionality would periodically send requests to M.E. Doc's public software update server for commands. These command requests initially were not answered.

On June 27, 2017, however, the threat actor modified the M.E. Doc update server to redirect the incoming command requests sent by computers running the compromised M.E. Doc software from the M.E. Doc server to another server controlled by the threat actor. The threat actor then centrally published on the attacker-controlled server a command to download and execute the destructive NotPetya payload. As a result, for a certain period of time on June 27, 2017, when computers running the compromised M.E. Doc software performed their periodic check-in with the M.E. Doc update server, they received the instructions to download and execute the NotPetya destructive malware.

NotPetya was a self-propagating, destructive malware, which means that it was a virus designed to automatically spread from computer to computer across a network. Once set loose into a network environment, NotPetya quickly spread, irreversibly locking computer files throughout the network using data encryption. Once the encryption was complete, the user was presented with a phony ransom message, instructing the user to pay $300 in Bitcoin to retrieve the locked information. In reality, there was no ransom or opportunity to recover the encrypted data. Rather, the infected computers were rendered permanently and completely unusable, essentially turning them into "bricks." Given the quick spread of the virus throughout a company's network, NotPetya affected computers not only in Ukraine, but crossed many national borders within hours.

II. INSURANCE CLAIMS

Several companies, including Merck (a pharmaceutical company based in New Jersey) and Mondelez (a snack company based in Illinois), submitted insurance claims to their property insurers for the damage to the computers and resulting loss of income. Although some property insurance policies provide coverage for physical damage to electronic data and software and loss of income caused by damage to computer systems, virtually all property insurance policies also include a "Hostile Acts Exclusion" (also known as a "War Risk Exclusion") which typically excludes "hostile or warlike action in time of peace or ware, including action in hindering combating or defending against an actual, impending or expected attack by any… government or sovereign power (de jure or de facto), … military, naval or air force; or … agent or authority [of the above]." Notably, while stand-alone cyber insurance policies oftentimes include a version of the Hostile Acts/War Risk Exclusion, those exclusions typically contain an exception or "carveback" for "acts of cyberterrorism," a phrase that has been defined as including an act of violence against the insured's computer system by an individual or group associated with a government.

III. WHO DUNNIT?

On February 15, 2018, approximately seven months after the NotPetya attack, the United States government formally, publicly, and unequivocally attributed NotPetya to the Russian military. The official White House pronouncement stated:

> In June 2017, the Russian military launched the most destructive and costly cyber-attack in history. The attack, dubbed "NotPetya," quickly spread worldwide, causing billions of dollars in damage across Europe, Asia, and the Americas. It was part of the Kremlin's ongoing effort to destabilize Ukraine and demonstrates ever more clearly Russia's involvement in the ongoing conflict. This was also a reckless and indiscriminate cyber-attack that will be met with international consequences.

The same week as the United States attribution, various other governments, including the United Kingdom, Australia, Canada, New Zealand, Denmark, Estonia and Lithuania, (and ultimately, Ukraine) released similar pronouncements attributing NotPetya to Russia. Thereafter, on March 15, 2018, the U.S. Government, through the Department of the Treasury's Office of Foreign Assets Control (OFAC), imposed sanctions on Russia for, among other things, "Russia's continuing destabilizing activities," including the NotPetya attack. Ultimately, the United States government indicted six officers in Russia's Main Intelligence and Directorate of the GRU (Russia's Chief Intelligence Office) for the officers' role in several high-profile cyberattacks, including NotPetya. See U.S. v. Andrienko, Case No. 20-316 (W.D. Pa. Oct. 15, 2020).

With the official government pronouncements that Russia and/or its military was behind the NotPetya attack, the property insurers took the position that the cost to repair the damage to their insureds' computers as a result of the NotPetya attack and the resulting loss of income were excluded from coverage by virtue of the Hostile Acts Exclusion. In this regard, the destructive cyber attack seemingly constituted a "hostile or warlike action in time of peace or war" by a "government or sovereign power." The NotPetya attack seemed to fall squarely within the

confines of the exclusion as a matter of undisputed fact. But, that is not what the courts determined.

IV. LEGAL PROCEEDINGS AND EXPERTS

So, what did the courts do when faced with the language of the exclusion in conjunction with the official government pronouncements? In the Merck action, the trial court determined that the Hostile Acts Exclusion applied only to "traditional forms of warfare" and did not include cyber attacks. That decision was appealed to the New Jersey Appellate Division, which concluded that the exclusion "requires the involvement of military action" and does not preclude "damages arising out of a government action motivated by ill will." Merck & Co., Inc. v. ACE American Ins. Co., 475 N.J. Super. 420, 436, 293 A.3d 535, 545 (2023)[1].

In the Mondelez action, the trial court did not rule out the possibility that a cyber attack could fall within the exclusion but determined that there was an issue of fact as to whether NotPetya was a "hostile or warlike act" and whether the attack was perpetrated by Russia (or any other nation state or military).

In Mondelez, the court also determined that the February 15, 2018 White House statement attributing the NotPetya attack to the Russian military was hearsay, i.e., an out-of-court statement offered for the truth of the matter asserted. This was so even though the insurers offered the testimony of Thomas P. Bossert, the President's Homeland Secretary Advisor at both the time of the NotPetya attack and the attribution by the United States. In connection with the United States attribution, his role was to coordinate all the relevant departments and agencies in the government, assisting in the drafting of the attribution statement, and ensure that the relevant cabinet secretaries and experts reviewed it and agreed to its phrasing. The insurer contended that the White House Statement fell within the public records exception to the hearsay rule and/or that the court could take judicial notice of the statement.

Nonetheless, the court in Mondelez determined that, because the attribution statement was based, in part, upon classified information to which Bossert could not testify and, as such, Mondelez could not fully cross examine Bossert regarding the basis for the government's attribution, the attribution statement was inadmissible hearsay. The court similarly declined to allow the insurer to submit into evidence the March 15, 2018 OFAC statement even though the Department of Treasury sanctions were issued pursuant to various legislative Acts and Executive Orders.

Given that the most direct and simple attribution of the NotPetya attack to the Russian military was ruled to be inadmissible evidence, the insurer was faced with having to prove the attribution to Russia through the use of multiple experts. These experts included: 1) **cyber attribution experts**, Laura Galante, the Director of the Cyber Threat Intelligence Integration Center, and Sean Kanuck, the former National Intelligence Officer for Cyber Issues on the National Intelligence Council, both of whom offered testimony that it was "very likely" or "almost certain" that the Russian military conducted the NotPetya cyberattack; 2) **experts in Russia/Ukraine relations**, including Dan Hoffman, CIA's former Moscow Station Chief, and

[1] Although the New Jersey Supreme Court granted review of the Appellate Division's decision, the case settled two days before oral argument was to take place.

Andrew Weiss, a former member of the National Security Council, Department of State, and Office of the Secretary of Defense, as well as Dr. Alina Polyakova, a renowned expert on Russia/Ukraine research, to address the military conflict between Russia and Ukraine that had been ongoing since 2014 with the invasion of Crimea and violence in the Donbass region of Ukraine; 3) **military experts**, including Vice Admiral Timothy White, who spent 33 years in the U.S. Navy and was Commander of U.S. Cyber Command, who testified regarding the changes in warfare to include cyber warfare in addition to more traditional methodologies of war; 4) **international law expert**, Gary Corn, who opined that the NotPetya attack was a hostile act under concepts of international law; and 5) **insurance expert**, Jason Schupp, to testify regarding the history of war exclusions in insurance policies.

V. THE FUTURE OF CYBER INSURANCE IN THE WAKE OF NOTPETYA AND LEGAL RULINGS

The question remaining is how to provide coverage to businesses for cyber attacks that are unrelated to a nation-state attack, while still excluding cyber attacks that are part of a war between nation states. The latter scenario presents significant accumulation risk for insurers that appropriate risk management dictates should be avoided. One possible solution is to specifically identify cyber warfare as a "hostile or warlike act." Notably, and as the insurers in Merck and Mondelez argued, there should be no need to identify every single action that could be considered "hostile or warlike" because the exclusion would become unwieldy in light of the fact that traditional notions of warfare continue to evolve. For instance, the exclusion currently does not identify any other specific modalities of war, such as "chemical warfare," "weapons of mass destruction," "airplane attack," or "naval attack." See, e.g., Tonoga Inc. v. New Hampshire Ins. Co., 159 N.Y.S.3d 252, 257 (3d Dept. 2022) (recognizing that damages resulting from broadly dispersed environmental harm fell squarely within pollution exclusions "regardless of whether a particular substance is specifically named as a pollutant in an insurance policy, whether a substance was understood to have a detrimental effect on the environment at the time the policy was entered into or whether the pollution was an intended result").

Other proposed solutions involve removing the attribution requirement of the exclusion. As seen from the rulings in Mondelez, insurers have an uphill battle in proving that a particular nation or its military was responsible for a cyber attack. If government pronouncements continue to be viewed as inadmissible hearsay, the only way to prove attribution is through the use of experts in the fields of cybersecurity, insurance, nation-state relations, international law, and military. Lloyds Market Association has begun drafting exclusions that no longer focus on the attribution of a cyber attack to a nation state or its military but rather, allow insurers to demonstrate attribution by "inference." One draft exclusion, for instance, states that "insurance does not cover that part of any loss, damage, liability, cost or expense of any kind… directly or indirectly arising from a war, and/or… arising from a cyber operation." The exclusion goes on to state that "[i]n determining attribution of a cyber operation to a state, the insured and insurer will consider such objectively reasonable evidence that is available to them. This may include formal or official attribution by the government of the state in which the computer system affected by the cyber operation is physically located to another state or those acting at its direction or under its control." It remains to be seen whether insureds will accept such policy wording.

The other issue insurers will be facing is how to avoid coverage for nation state cyber attacks while still providing coverage for more run-of-the-mill cyberattacks. In the Mondelez action, evidence was presented that underwriters at various companies were concerned with the implications of declining coverage for the NotPetya attack because other insureds and their brokers immediately assumed that cyber coverage, for which additional premium often is paid, would be rendered illusory. It will be the brokers' and underwriters' jobs to explain that, while coverage for cyber attacks is covered, cyber warfare by a nation state is not. It remains to be seen whether the solution will involve government underwriting similar to the Terrorism Risk Insurance Act ("TRIA") to address potential catastrophic worldwide disruptions in the market for cyber attacks undertaken by a nation state.