SUPREME COURT OF NEW JERSEY
Docket No. 088274

MERCK & CO., INC. and INTERNATIONAL INDEMNITY LTD., *Plaintiffs–Respondents*, v. ACE AMERICAN INSURANCE COMPANY; ALLIANZ GLOBAL RISKS US INSURANCE COMPANY; GENERAL SECURITY INDEMNITY COMPANY OF ARIZONA; HOUSTON CASUALTY COMPANY; LIBERTY MUTUAL FIRE INSURANCE COMPANY; LIBERTY MUTUAL INSURANCE COMPANY; QBE INSURANCE CORPORATION; SYNDICATE NOS. 609, 1183, 1200, 1686, 1886, 1919, 1955, 2003, 444, 4472, 5555 AND CONSORTIUM 9536 AT LLOYD'S LONDON; *(For Continuation of Caption, See Inside Cover)*	CIVIL ACTION ON MOTION FOR LEAVE TO APPEAL FROM AN INTERLOCUTORY ORDER OF THE SUPERIOR COURT OF NEW JERSEY, APPELLATE DIVISION DOCKET NOS. A-1879-21 A-1882-21 Sat Below: Hon. Heidi Willis Currier, P.J.A.D., Hon, Jessica R. Mayer, J.A.D., Hon Catherine I. Enright, J.A.D.

BRIEF FOR *AMICI CURIAE* EXPERTS IN INTERNATIONAL LAW AND THE LAW OF WAR IN SUPPORT OF MOTION FOR LEAVE TO APPEAL

On the Brief:
Michael Menapace (*pro hac vice* forthcoming)
WIGGIN AND DANA LLP
20 Church Street, 16th Floor
Hartford, CT 06103
Tel: (860) 297-3700
Fax: (860) 297-3799
mmenapace@wiggin.com

Susan M. Kennedy
WIGGIN AND DANA LLP
Two Liberty Place
50 S. 16th Street, Suite 2925
Philadelphia, PA 19102
Tel: (215) 988-8310
Fax: (215) 988-8314
skennedy@wiggin.com

Dated June 15, 2023

WESTPORT INSURANCE CORPORATION; XL INSURANCE AMERICA, INC.; ASSICURAZIONI GENERALI S.P.A.; HANNOVER RÜCK SE; HELVETIA SCHWEIZERISCHE VERSICHERUNGSGESELLSCHAF AG; MÜNCHENER RÜCKVERSICHERUNGS-GESELLSCHAFT,

Defendants.

ASPEN INSURANCE UK LIMITED; HDI GLOBAL INSURANCE COMPANY; NATIONAL UNION FIRE INSURANCE COMPANY OF PITTSBURGH, PA.; ZURICH AMERICAN INSURANCE COMPANY; MAPFRE GLOBAL RISKS, COMPAÑIA INTERNACIONAL DE SEGUROS Y REASUGUROS S.A.; VIENNA INSURANCE GROUP AG,

Defendants–Appellants.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Other Authorities

Preliminary Statement

The Amici Experts understand that Insurer Defendants ("Insurers") have filed a petition for certification for leave to appeal in this matter. Insurers' motion for leave has been filed under seal and Amici Experts are not privy to that motion. Nevertheless, the Amici Experts ask this Court to accept review of the Appellate Division Opinion, dated May 1, 2023 (the "Decision") for two reasons.

First, the Decision did not recognize the realities of modern warfare and the use of cyber technology in modern-day conflicts between nation states. Similar to international law, courts must adapt legal doctrines designed to address the inherent risks of warfare to account for new technologies and means and methods of armed conflict. Failure to consider these realities risks establishing incongruent precedent. Second, the Appellate Division's statements dismissing the notion that the NotPetya attack had anything to do with armed conflict are fundamentally wrong both factually and as a matter of international law.

The New Jersey Superior Court and the Appellate Division short-circuited the fact-finding process in this insurance coverage dispute, leading to unsupported and factually infirm findings. In affirming summary judgment, the Appellate Division relied on several assumed facts that are, in actuality, not true, and then compounded its error by misstating international law as it relates to cyber operations and warfare. By essentially characterizing NotPetya as a cyberattack

against a non-combatant that impacted other non-combatants "wholly outside the context of any armed conflict or military objective," the Decision minimizes the serious nature of modern cyber operations conducted by nation states (and/or their militaries) and risks perpetuating confusion as to the application of the international law of armed conflict ("LOAC").

Accordingly, the Amici Experts support the Insurers' request for review of the Decision. Ultimately, the Amici Experts advocate for remanding this dispute to the trial court so that facts about the NotPetya cyberattack can be properly considered, including the relevant context of the state of international armed conflict that existed between Russia and Ukraine in 2017 when the Russian military launched NotPetya, and whether such use of a modern means and method of warfare, regulated as such by international law, constitutes a hostile or warlike act.

Here, there is an abundance of evidence to demonstrate that the launch of NotPetya was undertaken by the Russian military in the context of an ongoing military conflict with Ukraine. The use of destructive and disruptive encryption malware against a wide array of government and civilian targets in Ukraine as part of that ongoing conflict was a means and method of warfare regulated by the LOAC. The Amici Expert's interest here is to ensure that international law is stated

correctly and that the Appellate Division's categorical and premature rejection that NotPetya could be a hostile or warlike act be reviewed.

Identity and Interest of Amici Curiae

The proposed Amici Experts are former officials of the U.S. Department of Justice, U.S. Department of Defense, U.S. Department of Homeland Security, and U.S. Cyber Command. They have held senior government positions, are international law scholars, and have taught at the College of Information and Cyberspace (the U.S. Cyber War College).[1]

This appeal presents important questions that require an accurate statement of international law as it relates to cyber activities. Respectfully, the Appellate Division misconstrued the nature, context, and origin of NotPetya. Further it misstated international law and the law of war, as well as the United States' official view as to the applicability of international law to cyber operations. The Amici Experts have an interest in the proper characterization the NotPetya cyber operation and application of international law and the law of war as it relates to cyber activities conducted in the context of an ongoing armed conflict.

[1] The references to the Amici Experts' current positions are for identification and disclosure only. The views expressed in the proposed brief of the amici are their individual roles and are not intended to be representations by their current employers.

Brandon J. Pugh serves as the director and resident senior fellow for the R Street Institute's Cybersecurity and Emerging Threats team. He also serves as an international law officer in the U.S. Army Reserve and as a non-resident fellow with the Army Cyber Institute. He has served on the cybersecurity program advisory boards for both Rutgers University and Ithaca College. Previously, Brandon served as legislative counsel for the New Jersey General Assembly (Minority Office), as Managing Editor for the Journal of Law & Cyber Warfare, and in elected and/or appointed office at the local, county, and state level in New Jersey.

Paul Rosenzweig served as the first Deputy Assistant Secretary for Policy at the Department of Homeland Security, where he participated in the development of the first Comprehensive National Cybersecurity Initiative. He teaches at George Washington University School of Law and is a Senior Fellow at the Tech, Law & Security Program at the Washington College of Law, American University. He currently serves as a member of the American Bar Association, Cybersecurity Task Force and has lectured on issues relating to the application of the Laws of Armed Conflict to Cyberspace at the Judge Advocate General's Legal Center and at U.S. Cyber Command.

Kurt Sanger, Lieutenant Colonel, U.S. Marine Corps (Ret.) served as an attorney for U.S. Cyber Command for eight years, finishing as the Command's Deputy

General Counsel. He has taught at National Defense University, Marine Corps University, Campbell University, and guest lectured at multiple law schools, undergraduate institutions, and military academies. He is the founder and director of Integrated Cybersecurity Partners, LLC, a cyber and national security consultancy. Lieutenant Colonel Sanger helped draft, edit, and advocate for the most significant executive branch policies, strategies, directives, regulations, orders, and doctrinal publications regarding cyberspace operations from 2014-2022, as well as related legislative proposals.

Cory Simpson has significant experience in government, the military, and the private sector at the intersection of national security, cybersecurity, law, and strategy. Atty. Simpson has served in multiple legal and operational roles within USCYBERCOM and the National Security Agency focused on the offensive use of cyber and information warfare capabilities. He also served as a senior director for the U.S. Cyberspace Solarium Commission—a bipartisan, bicameral, intragovernmental commission that left a historical impact on US government cyber policy and strategy. Today, Cory is the founder and CEO of Gray Space Strategies, a professional service and strategic advisory firm in Washington, D.C.; a senior advisor to the CSC 2.0—a non-profit and non-partisan entity that continues the work of the U.S. Cyberspace Solarium Commission; an adjunct senior fellow in the National Security and Technology program at the Center for

New American Security; and an adjunct professor at Clemson University teaching cybersecurity and homeland security policy.

Thomas C. Wingfield is a Senior Defense and International Researcher at the RAND Corporation in Washington, DC. Previously, he served as the Deputy Assistant Secretary of Defense for Cyber Policy from 2019 to 2021. Prior to that, Mr. Wingfield was the Dean and Acting Chancellor of the National Defense University College of Information and Cyberspace, the nation's cyber and information war college. He holds a J.D. and an LL.M. from Georgetown University Law Center. A former Chair of the American Bar Association's Committee on International Criminal Law, he is the author of THE LAW OF INFORMATION CONFLICT: NATIONAL SECURITY LAW IN CYBERSPACE and a drafter of the TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (discussed below)

Analysis

The Appellate Division concluded that there is a requirement of military action for damages to be considered the result of hostile or warlike action by a government or sovereign power in times of war or peace. Decision, p. 20. The Appellate Division further concluded that the NotPetya attack was "wholly outside the context of any armed conflict or military objective," despite the overwhelming evidence that NotPetya was conducted by the Russian military in furtherance of its ongoing armed conflict with Ukraine. Decision, p. 23.[2] Ultimately, the Appellate Division categorically held that the hostile or war-like act exclusion could not apply to a cyberattack on a non-military company that provided accounting software for commercial purposes to non-military consumers. Decision, p. 24. This conclusion was based on an incorrect factual understanding of the nature of the NotPetya attack, which was directed at and resulted in significant harm to

[2] The Appellate Division also looked to case law that pre-dated cyber warfare. *See* Decision, pp. 25-35. But pre-cyber era case law cannot serve as evidence that U.S. law does not recognize cyberattacks as part of warfare. In any event, the pre-cyber era case law demonstrates that acts of destruction in the context of an ongoing military conflict can, indeed, be considered a "hostile act by or against a belligerent power…." *Int'l Dairy Engineering Co. v. Am. Home Assur. Co.*, 352 F. Supp. 827 (N.D. Cal. 1970), *aff'd* 474 F.2d 1242 (9th Cir. 1973) (a flare drop during the Vietnam War, which accidentally drifted over to the insured's processing plant and started a fire, was excluded under a provision precluding coverage for "fire … caused directly … by a hostile act by or against a belligerent power…," even though the flare was not designed as a use of armed force that was intended to cause harm or destruction).

Ukraine and companies doing business in Ukraine during the course of an ongoing military conflict, rather than directed at an accounting software company.

A. Hostile Cyber Operations Conducted in the Context of Armed Conflict Qualify as Means and Methods of Warfare under the International Law of Armed Conflict

The Decision, in concluding that a cyberattack such as NotPetya is not a hostile act makes several incorrect statements of international law.

Under international law and, in particular, the LOAC, once two nations such as Russia and Ukraine are engaged in armed conflict, the tools they use and the operations they conduct in the furtherance of their hostilities constitute means and methods of warfare regulated by the LOAC and, by extension, "hostile" or "warlike" acts. There is no doubt that the belligerent occupation of eastern Ukraine in 2014 by Russian forces, as well as the deployment of tanks, artillery systems, and up to 50,000 troops on the Russia-Ukraine border, constituted the initiation of an "armed conflict" under international law that Russia has prosecuted continuously until the present. Indeed, the White House recognized this fact in its February 15, 2018 Statement, stating that the NotPetya attack was "part of the Kremlin's ongoing effort to destabilize Ukraine and demonstrates ever more clearly Russia's involvement *in the ongoing conflict*." (Emphasis added.)

In the case of an ongoing armed conflict against another nation state, as is the case here, international law is clear -- destructive cyberattacks launched by the

military of a nation state in the course of its ongoing armed conflict against another nation state, including against civilians and civilian objects and infrastructure (including computers, networks, and other cyber infrastructure), are means and methods of warfare subject to LOAC application. They present the same "circumstances [as other military operations] in which it is impossible to evaluate the risks" of liability traditionally excluded as hostile or warlike acts. *Diamond Shamrock Chems. Co. v. Aetna Cas. & Sur. Co.*, 258 N.J. Super. 167, 231 (App. Div. 1992).

Warfare has evolved to encompass new means and methods. For example, the United States Department of Defense Law of War Manual, June 2015 (updated Dec. 2016), Chapter XVI, addresses Cyber Operations. That manual provides, in part: "As a matter of U.S. policy, the United States has sought to work internationally to clarify how existing international law and norms, including law of war principles, apply to cyber operations." The DOD Law of War Manual further makes clear that "[s]pecific law of war rules may apply to cyber operations, even though those rules were developed before cyber operations were possible." Law of War Manual, Section 16.2.[3] More specifically, Section 16.5 makes emphatically clear the United States' view that the *jus in bello* (the body of

[3] The DOD Law of War Manual may be found here. DoD-Law-of-War-Manual-June-2015-Updated-May-2016.pdf (documentcloud.org)

international law that regulates how parties to an armed conflict engage in hostilities, i.e. LOAC), applies to cyber operations.

Since at least 2012, the U.S. has been emphatic in its view that international law, including LOAC, applies to states' activities in cyberspace and specifically that, "in the context of armed conflict, the law of armed conflict applies to regulate the use of cyber tools in hostilities, just as it does other tools." Koh Speech at Cyber Command. The United States has reiterated and detailed this view numerous times, including in the Department of Defense ("DOD") Law of War Manual as well as in its official submissions to the UN. *See* United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security ("UN GGE"), 2021 UN GGE report, para. 71 (a) – (g).[4]

In the case of NotPetya, the malware caused the infected computers to become inoperable and useless (as demonstrated by the Plaintiff filing a property insurance claim that required "direct physical loss of or damage to property"). If a bomb or missile damaged or destroyed these computers, rendering them inoperable and useless, there is no doubt that the event could be categorized as a hostile or war-like act. And, there would be no meaningful difference on the impacted

[4] The UN GGE report can be found here. A_76_135-2104030E-1.pdf (un-arm.org)

computers if they were owned by private individuals/businesses and were collateral damage, not the primary target, of the intended near-by explosion. A cyberattack that produces collateral damage on connected computer systems can be similarly categorized as a hostile/war-like act under international law.

Just like the U.S. Department of Defense, the U.S. State Department has taken the public position – still in effect – that cyberattacks are elements of armed conflict regardless of whether they have kinetic or non-kinetic effects. *Use of Force in Cyberspace*, Congressional Research Service Report, 12-10-2021.[5]

That cyberattacks are a part of modern warfare has been recognized by numerous states and is well accepted among international law scholars. In 2009, an independent group of twenty international experts on international law and the law of war met at the request of NATO in order to produce a manual on the international law governing cyber warfare. The focus of the resulting manual, entitled *Tallinn Manual*, published in 2013, was on both "cyber operations involving the use of force and those that occur in the context of armed conflict." It is a seminal work and addresses how to interpret international law in the context of cyber operations. In 2017, the second edition of the *Tallinn Manual* (*Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*) expanded on the first edition by extending its coverage of the international law governing

[5] Available at https://crsreports.congress.gov

cyber warfare to, among other things, peacetime legal regimes Page 451 of *Tallinn Manual 2.0* cites to paragraph 86 of the International Court of Justice's July 8, 1996 Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, which stated that the "established principles and rules of humanitarian law…appl[y] to all forms of warfare, and *to all kinds of weapons, those of the past, those of the present and those of the future.*"

The holdings of the trial court and Appellate Division that a cyberattack on a non-military company that provided accounting software for commercial purposes to non-military consumers (Decision, p. 24) cannot be "hostile or warlike" is simply incorrect as a matter of fact and law, and sets a dangerous precedent. As set forth in the *Tallinn Manual 2.0*, in determining whether an act constitutes a means and method of warfare, the court must be flexible enough to incorporate new technology that is used in modern warfare. Thus, the Appellate Division gave short shrift to the realities of NotPetya and what the implications are for future attacks.

Equally important, the Appellate Division's holding suggests that an attack on non-military consumers, even if undertaken by a government or sovereign power, cannot be "hostile or warlike." But, using tools and weapons and other means and methods of warfare that harm civilian targets is *exactly* what the LOAC is meant to address and prevent. In the case of NotPetya, the fact that non-military

businesses and civilians, in addition to government entities, were harmed is precisely what the LOAC proscribes. Indeed, cyber operations like NotPetya can form the basis of war crimes charges, and is exactly why the UC Berkeley School of Law's Human Rights Center has urged the International Criminal Court to investigate and prosecute the perpetrators of the NotPetya operation.

B. The Appellate Division's Finding that NotPetya Had Nothing to Do with Armed Conflict is Fundamentally Wrong Both Factually and as a Matter of International Law

The Appellate Division held that the hostile or warlike act exclusion "did not include a cyberattack on a non-military company that provided accounting software for commercial purposes to non-military consumers, regardless of whether the attack was instigated by a private actor or a 'government or sovereign power.'" Decision, p. 24. However, whether NotPetya occurred in the context of armed conflict or as part of a military objective is at best a disputed issue of material fact. Indeed, as addressed above, the weight of available evidence demonstrates that NotPetya took place in the context of an ongoing military conflict between two nation states.

The Appellate Division started down the wrong path with a basic misunderstanding of cyber operational methodologies generally and of NotPetya specifically. NotPetya did not "target" the accounting firm, M.E. Doc. The Russian forces coopted and employed M.E. Doc software to affect a broader set of

Ukrainian targets. *See* Unsealed Indictment filed in *United States of America v. Andrienko*, No. 20-315, W.D. Pa. (Oct. 15, 2020) at ¶¶ 34-37(stating that the GRU disseminated the NotPetya malware using a popular Ukrainian accounting software, causing damage to other victims using that software). The strategic value of targeting M.E. Doc as an organization was negligible, but its software's value as a conduit to impact a broader set of Ukrainian military and government organizations, as well as its economy and ability to support its defense, is easily apparent. This is the true "context" the Appellate Division should have considered.

The Appellate Division compounded its initial misunderstanding by misstating the purpose and origin of NotPetya. The Appellate Division stated: "Here, the NotPetya attack is not sufficiently linked to a military action or objective as it was a non-military cyberattack against an accounting software provider." Decision, pp. 34-35. First, multiple credible sources, including the U.S. Department of Justice and several nation states, have attributed NotPetya not just to Russia, but specifically to the GRU—Russia's military intelligence agency. Second, the Appellate Division's "sufficiency" phrase begs for a fact-finding inquiry.

The Amici Experts acknowledge that the Plaintiff and others might assert that NotPetya was not a military action or that the primary target was accounting

software, but the disagreement on those issues among the parties to this litigation only goes to demonstrate that this issue is not appropriate for summary judgment. As noted, it is widely understood that a Russian military organization, the GRU, conducted NotPetya as part of an ongoing conflict between Russia and Ukraine. It was not something akin to a random cyberattack on private companies for the purpose of monetary profit. Indeed, the effects of NotPetya could not be reversed or mitigated by the payment of any sort of ransom. There is significant evidence for the conclusion that NotPetya was a military cyber operation intended to harm Ukraine and advance Russia's strategic war aims.

Further, the Appellate Division incorrectly concluded that the NotPetya attack occurred "wholly outside the context of any armed conflict or military objective." Decision, p. 23. As addressed above, since one party to an armed conflict, Russia, launched this attack against the other party to the armed conflict, Ukraine, during the period of hostilities, this conclusion is factually incorrect and, at the very least, should be determined by a factfinder.

The Amici Experts are not asking this Court to decide attribution and/or the strategic intention behind NotPetya at this stage of the proceeding. They simply ask that this Court recognize that there is more than enough evidence to establish that full fact-finding could result in a finding that NotPetya was an operation of the Russian state undertaken as part of its ongoing conflict against Ukraine. Indeed,

on March 15, 2018, the U.S. Government issued sanctions against Russia for "Russia's continuing destabilizing activities, ranging from interference in the 2016 elections to conducting destructive cyber-attacks, including the NotPetya attack, a cyber-attack attributed to the Russian military on February 15, 2018 in statements released by the White House and British Government." Moreover, as noted above, the DOJ filed an indictment against six officers in Military Unit 74455 of the Russian GRU. In addition, there was ample evidence cited by the Appellate Division that NotPetya was orchestrated by Russia. Decision, p. 10 (Insurers' consultant, Kroll, concluded "with high confidence, that the NotPetya cyber-attack was very likely orchestrated by actors working for or on behalf of the Russian Federation.").[6]

The Decision, affirming a premature summary judgment ruling did not fully consider that the target of NotPetya was the Ukrainian economy and Ukraine's ability to (i) finance its military opposition to Russian forces and (ii) maintain esprit de corps and morale amongst its armed forces and civilians.

Conclusion

The Amici Experts ask the Court to grant the Insurers' motion to review the Decision. This dispute should ultimately be remanded to the trial court for a

[6] *See also* Pavel Polityuk, *Ukraine points finger at Russian security services in recent cyber attack*, Reuters, July 1, 2017 (Ukraine blaming the NotPetya attack on Russia).

decision after the opportunity for facts to be considered and a full record. The trial court's full consideration would include attribution of NotPetya, the GRU's structure and operations, the NotPetya attack methodology, intended targets (such as Ukraine's financial systems, government departments and agencies, critical infrastructure and private-sector operations and services), and intended strategic outcomes to support Russia's overall war aims. Most important, the Appellate Division's decision, as it currently stands, risks dangerous precedent in not recognizing the modern-day concepts of hostilities and war, and includes incorrect factual statements concerning the nature of the NotPetya attack.

Dated: June 15, 2023

Respectfully submitted,

/s/ *Susan Kennedy*

Susan Kennedy, Esq.
Wiggin and Dana, LLP
Two Liberty Place
50 S. 16th Street, Suite 2925
Philadelphia, PA, 19102
215-988-8319
skennedy@wiggin.com

Michael Menapace, Esq. (*pro hac vice* forthcoming)
Wiggin And Dana LLP
20 Church Street, 16th Floor
Hartford, CT 06103
(860) 297-3700
mmenapace@wiggin.com

Attorneys for the *Amici Curiae* Experts in International Law and The Law of War