When Security Paradigms Fail

By Roland L. Trope[*]

I. Introduction

This survey addresses developments during the year in review that arose from a company's misplaced reliance on a flawed or obsolete "security paradigm" and the adverse consequences that resulted.

The term "security paradigm" refers to a set of operating assumptions, concepts, and practices with respect to external and internal threats to a government's or enterprise's security and the capabilities needed to protect and defend against such threats. Threats to a government's or enterprise's security paradigm may take the form of cyberattacks, robot malfunctions, or errors in design or programming that create security threats to operations or personnel.

In the Digital Era, security threats—external and internal—shift continuously. At certain points, a latent or emergent threat may subvert the existing security strategies. When that happens, a shift in the security paradigm starts. The shift ends when the government or enterprise adapts a security paradigm to protect against the latent or emergent threat. Adapting a security paradigm refers to "changes in previously held assumptions about values, actors, interests, threats and capabilities that no longer adequately explain the security environment."[1]

Security paradigms often endure beyond events that exploit their flaws or obsolescence. Governments and enterprises often do not recognize when a prevailing security paradigm was incurably flawed from its inception or has neared the end of its efficacy. Mishaps may highlight a security paradigm's inherent flaws or foreshadow its diminished effectiveness. Mishaps, if not catastrophic, tend to be dismissed, be undeserving of our attention, or involve acceptable trade-offs. There are, however, mishaps that jolt us either by the prodigious cost in damage to tangible structures and intangible data or by the harm done to humans.

[*] Roland L. Trope is a partner at Trope and Schramm LLP in New York City and an Adjunct Professor in the Department of Electrical Engineering and Computer Science at the U.S. Military Academy at West Point. He can be contacted at rltrope@tropelaw.com.

Disclaimer: The views expressed herein are solely the author's and should not be attributed to the U.S. Military Academy, the U.S. Department of the Army, the U.S. Department of Defense, or the U.S. Government.

The author thanks John Rothchild and Winston Trope for editing, and Benjamin Bejster for cite checking and bluebooking the essay.

[1] Roy Godson & Richard Shultz, Adapting America's Security Paradigm and Security Agenda 33 (2010), https://apps.dtic.mil/sti/pdfs/ADA516785.pdf.

Regrettably, it often takes a severe mishap to compel officials and officers to recognize that a security paradigm should no longer be relied upon—even if we do not have, ready at hand, a better one to put in its place. And if relinquishing the security paradigm only addresses the cause of the mishap, but overlooks cybersecurity threats and risks, the risk of harm remains and may not even be diminished.

During the year in review, governments and enterprises had to reckon with misplaced reliance on flawed and obsolete security paradigms. In this survey, we look at two security paradigms that underwent judicial re-examination and that may have been discredited, but nonetheless remain vulnerable to serious risks from cyber bad actors.

Part II of this survey examines a security paradigm involving autonomous robots and humans. The paradigm assumes that autonomous robots, lacking human safeguards, can be relied upon to operate safely in close proximity to humans. This security paradigm tends to overlook the possibility that robot malfunction or errant programming of the robot controller may occur at the same time and place as errors or mistakes by human co-workers. This security paradigm's flaw became apparent in a decision that the U.S. District Court for the Western District of Michigan issued on September 20, 2021, in *Holbrook v. Prodomax Automation Ltd.*[2]

Part III of this survey examines a security paradigm that a drafter of a cyber insurance exclusion clause appeared to rely upon when the drafter refrained from revising a policy to address an emergent cyber technology and the potential "warlike" use of the cyber technology in an armed conflict. The security paradigm of interest is the drafter's apparent presumption that the insurance policy's "warlike action" exclusion clause will be interpreted the same by insurer and insured: that is to say, without any need for the insurer to propose new language to clarify the scope of the policy in light of a belligerent's potential use of the new cyber technology for warlike activities. The security paradigm presumes that contract language will "auto-update" to address emergent digital security risks, even when the language clearly fails to address such risk. This security paradigm's obsolescence became apparent in a decision that the Superior Court of New Jersey issued on December 6, 2021, in *Merck & Co. v. Ace American Insurance Co.*[3]

II. *Holbrook v. Prodomax Automation Ltd.*

A. Facts

Prior to July 2015, Ford Motor Company ("Ford") contracted with Flex-N-Gate ("FNG") to supply trailer hitch receiver assemblies for Ford's F-150 pickup trucks. FNG contracted with Prodomax Automation, Inc. ("Prodomax") to design, build, and install assembly lines of autonomous robots that would manufacture

[2] No. 1:17-cv-219, 2021 WL 4260622 (W.D. Mich. Sept. 20, 2021).

[3] No. UNN-L-002682-18, 2022 WL 951154 (N.J. Super. Ct. Jan. 13, 2022).

the hitch receivers at the Ventra Ionia plant, which was operated by an affiliate of FNG in Ionia, Michigan (about 130 miles northwest of Detroit). FNG purchased the robots from a Japanese robot-maker and its U.S. subsidiary. Ford contracted with Prodomax to make automated assembly lines utilize the robots.[4]

At the Ventra Ionia plant, the assembly line robots operated within six enclosed zones demarcated by retractable walls. Each robot's zone could be accessed by a door in the retractable walls. In each zone, a robot performed a portion of making a trailer hitch receiver[5] assembly.[6]

Although autonomous, and programmed for 24/7 operation, the robots occasionally required human co-workers to enter a robot's zone to perform maintenance. Since the robots' fast operation posed dangers to humans, the factory implemented mandatory procedures to ensure a human's safe entry into, work within, and departure from each robot's door-accessible zone. The procedural steps were:[7]

- A human presses a "request to enter button" outside a zone's door;
- The robots in the zone cease operating;
- At the same time, the zone's wall rises to ensure robots operating in other zones cannot enter;
- A green light appears, signaling to humans they may safely enter the halted robot's zone;
- The human places a tagged safety lock on the zone's door on entry to prevent it from closing because an open door prevented the zone's robot from resuming autonomous operation and kept robots in adjacent zones from entering the human occupied zone.

The robot assembly line contained three zones relevant to the case:

(i) Zone 130, whose robot placed a hitch assembly in two fixtures located in Zone 140;

(ii) Zone 140, whose robot welded each hitch assembly; and,

(iii) Zone 150, whose robot extracted and transferred the welded hitch assembly to a cooling site.

On July 7, 2015, a zone 130 robot inserted a hitch assembly into the fixture for welding; a zone 140 robot welded the hitch assembly; and a zone 150 robot

[4] *Holbrook*, 2021 WL 4260622, at *1.

[5] A trailer hitch receiver is the primary connector between a pickup truck and trailer; the receiver hitch "bolts onto the underside of the vehicle, at the rear, and provides a tube for attaching a ball mount or other hitch accessory . . . . [And] generally have a vehicle-specific design . . . ." *Parts of a Trailer Hitch*, Curt Mfg., https://www.curtmfg.com/basic-towing-components (last visited July 10, 2022). To view an example of the hitch receiver for the Ford-150 pickup (circa 2009–2014), see https://accessories.ford.com/products/f-150-2009-2014-black-trailer-hitch-assembly-2-receiver-1.

[6] *Id.* at *2.

[7] *Id.*

reached over the lowered retractable wall (between zones 150 and 140) and attempted unsuccessfully to pick up the welded hitch assembly. The zone robot 150 could not grab and extract the hitch assembly because the hitch, as welded, was misaligned in the fixture.[8] While not clear from the court's description, robot malfunctions may have caused the misalignment (in placement, welding, or both). Thwarted, the zone 150 robot defaulted to inactivity and "lay stretched across the lowered [retractable] wall between zones 140[, containing the misaligned hitch,] and 150."[9]

Apparently, factory protocol required a human to intervene to restore operations when a robot defaulted. In this instance, Wanda Holbrook, a maintenance technician, followed the required procedures for entry into zone 150, where she picked up the defaulted robot's wired control panel. She then apparently decided to enter the adjacent zone 140, containing the misaligned welded hitch. But instead of following the required procedures for entry into that adjacent zone—and thereby deactivating zone 140's welding robot—she inexplicably climbed over the lowered retractable wall to go from zone 150 to zone 140. She used the wired control panel to move the powered-down zone 150 robot out of the way.[10]

Unfortunately, the zone 140 robot's sensor malfunctioned. It falsely detected an empty fixture and powered up to deliver another hitch to the fixture for welding. The zone 130 robot entered zone 140 with a new hitch assembly. The zone 130 robot's sensitive sensor had not been programmed to detect obstacles in its path (an additional flaw in the robots). The zone 130 robot proceeded with the hitch assembly toward the empty fixture, crushed Wanda's head, and pinned her in zone 140 between the new hitch assembly and the welded misaligned hitch assembly.[11] Robots in zone 140 then "attempted to weld the new hitch assembly, severely burning Wanda's 'face, nose, and mouth.'"[12] The combined actions of the robots killed Wanda.[13]

Within hours of the accident, Prodomax reprogrammed the assembly line's programmable logic controller ("PLC") so that opening one zone's door would cause robots in all zones to power down.[14] Thus, Prodomax appeared to have recognized that the security paradigms it relied upon to safeguard humans working with robots were inherently flawed.

B. Accountability for Robot Harm to a Human Co-Worker

Wanda's husband, William Holbrook, acting as personal representative of her estate, filed wrongful death actions against multiple parties based on common law negligence and product liability. Eventually, two defendants remained: FNG

[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] *Id.* at *3.
[14] *Id.*

(which procured the robots) and Prodomax (which organized the robots into an assembly line). Defendants moved for summary judgment and judgment on the pleadings.[15]

Plaintiff alleged that Prodomax negligently programmed the robotic assembly line. Plaintiff pointed to the fact that within hours of the accident, Prodomax reprogrammed the PLC so that anytime someone opened a single zone's door, robots in every zone would power down. Plaintiff argued that Prodomax's pre-accident decision to program the PLC to trigger zone-specific shutdowns was negligent and that the system should have been programmed for all-zone shutdowns as Prodomax did post-accident.[16]

Defendants argued that since the PLC programming was a "product," the Michigan Product Liability Statute ("MPLS"), which provided the sole remedy for product liability claims, required dismissal of the common law negligence action.[17] The district court noted that the Michigan Supreme Court had not addressed whether software, such as the PLC programming, should be considered a product, and no lower state courts had addressed the issue. The district court therefore addressed the issue by anticipating how Michigan courts would answer the question.[18] Based on the MPLS's definition of "product," and the dictionary definition of the term, the court held that both the assembly line and the PLC programming were products and that, therefore, the MPLS, not the common law, governed the plaintiff's action.[19]

In reaching that conclusion, the district court addressed the plaintiff's contention that programming caused the accident and that programming "cannot possibly be part of the design" because programming of the assembly line of robots was not completed until installation at the factory. In rejecting that argument, the district court reasoned:

> [T]he PLC programming determines how the [set of robots] functions *as an assembly line*: it tells the many robots when to act, or not, and, crucially, it determines how much of the [assembly line] would remain in operation while portions of the line were under maintenance. The PLC programming determines how the [set of robots] functions; that falls squarely within "design."[20]

The district court thus agreed with the defendants' argument that the PLC programming is part of the *design* of the assembly line.[21] The district court explained that plaintiff's allegation of negligent programming of the PLC amounted to alleging a defectively designed product, which would be governed by the MPLS and could not be brought as a common law negligence action. Since the parties agreed that FNG "does not qualify as a manufacturer or non-manufacturing

[15] *Id.* at *1, *3.
[16] *Id.* at *4.
[17] *Id.*
[18] *Id.* at *5.
[19] *Id.*
[20] *Id.* at *6.
[21] *Id.*

seller under the MPLS," the district court granted FNG's motion for summary judgment.[22]

The district court, however, declined to grant Prodomax's motion for summary judgment on plaintiff's product liability claim. Prodomax argued that it was shielded by a provision of the MPLS stating that a manufacturer is not liable in product liability for "'harm caused by misuse of a product unless the misuse was reasonably foreseeable.'"[23] But the district court concluded that Wanda's misuse of the robot assembly line (i.e., disregarding the safety protocols and climbing over the lowered retractable wall between two zones of operating robots) was demonstrably foreseeable, because Prodomax had indeed foreseen it, as evidenced by testimony of a Prodomax engineer that the purpose of the retractable wall "even when lowered, was to 'prevent a person from' going between zones in the exact way that Wanda did."[24] Moreover, the district court did not rule that the programming alone was a "product," and instead pointed out that "programming need not qualify as a product itself."[25]

C. Flaws in the Robot/Human Security Paradigm

Although the district court does not expressly say so, its reasoning reveals that Prodomax relied upon a digital security paradigm that was both flawed and obsolete. Prodomax's quick reprogramming of the PLC from zone-shutdowns to entire assembly line shutdown suggests that Prodomax may well have considered programming the PLCs that way from the outset. Doing so, however, would have made the assembly line less efficient and profitable: each time a robot needed "in zone" human adjustment or maintenance, the entire assembly line would have to shut down.

Thus, human error by a worker was foreseeable. So, too, was programming the PLC to diminish the probability that such accidents could occur. Prodomax had relied on a flawed security paradigm. But its security paradigm was probably also obsolete back in 2015 when the accident occurred, which Prodomax should have recognized. Evidence of its obsolescence had been accumulating for years. The evidence appeared a year earlier, in a 2014 *New York Times* article that recounted some of the thirty-three robot-caused U.S. workplace deaths. One such accident occurred in March 2006, at a car factory, where "[a] robot caught an employee on the back of her neck and pinned her head between itself and the part she was welding" and killed her.[26] As the district court noted, these robots when "operating in full swing . . . are fast and dangerous."[27] It did not require deep analysis or a grasp of robotics complexities for a designer to recognize that

[22] *Id.* at *7.

[23] *Id.* (quoting Mich. Comp. Laws § 600.2947(2)).

[24] *Id.* at *8.

[25] *Id.* at *6.

[26] John Markoff & Claire Cain Miller, *As Robotics Advances, Worries of Killer Robots Rise*, N.Y. Times (June 16, 2014), https://www.nytimes.com/2014/06/17/upshot/danger-robots-working.html?_r=0.

[27] *Holbrook*, 2021 WL 4260622, at *2.

error-prone humans will not be as strict as robots in adhering to rules. And a few minutes of research would have revealed several instances where humans had been killed in accidents involving robots in the workplace.

D. Digital Security Lessons

Three digital security lessons may be drawn from *Holbrook*.

First, when a sequence of robot malfunctions and human errors cause injury to, or death of, humans, we tend to forgive the humans, but not the robots. Our unwillingness to forgive the robots extends to the humans who decided on how the robots would be programmed. Hence, one of the most entrenched security paradigms is the insistence that liability for robot harm done to humans be traced back to humans who made decisions that let it happen.

Second, companies that design or purchase robots to work with humans should foresee the harm that can arise from a combination of robot malfunction, human error, and placement of humans and robots in close proximity. Neither the robot designer nor the robot purchaser-user should implement security paradigms that rely on error-prone humans' adherence to safety protocols. The designer could instead program the robots to practice the first of Isaac Asimov's *Three Laws of Robotics*: "a robot may not injure a human being, or, through inaction, allow a human being to come to harm."[28]

Third, Prodomax's post-accident reprogramming of the robot assembly line would shift reliance away from the security paradigm that puts excessive trust in error-prone humans to adhere to safety protocols. Reprogramming for improved safety, however, is a reversible action: cyber attackers can hack into a company's operational computers and reprogram the robots to malfunction like those in *Holbrook*. Bad actors (whether outsiders or insiders) can re-program robots to perform poorly (as in the misalignment of the welded hitch assembly) or to malfunction (as in the robot sensor that erroneously detected an empty assembly). If a robot can be programmed to enhance safety, it can be hacked and reprogrammed to enhance the robot's abilities to damage equipment, disrupt operations, and maim or kill human co-workers. As government and commercial reliance on robots and AI-augmented machines rapidly increases, counsel should consider alerting its government and commercial clients of the need for commensurate enhancements of cyber security.

Cyber threats from a belligerent state (and its sponsored bad actors) became imminent once Russia's armed forces invaded Ukraine in February 2022. Confirmation of the threat appeared in a joint alert issued on May 9, 2022, by the U.S. Cybersecurity & Infrastructure Security Agency and the cybersecurity authorities of the other "five eyes" allies (Australia, New Zealand, Canada, and the UK).

[28] Isaac Asimov, *Runaround*, Williams Coll., https://web.williams.edu/Mathematics/sjmiller/public_html/105Sp10/handouts/Runaround.html (last visited July 10, 2022); *see also Three Laws of Robotics*, Britannica.com, https://www.britannica.com/topic/Three-Laws-of-Robotics (last visited July 10, 2022).

Such threats, however, are not limited to direct cyberattacks, but may emerge as collateral damage from malware released by Russia as part of its belligerent activities against Ukraine's sovereignty. Cyberattack collateral damage from reportedly Russia-sponsored hackers gave rise to the insurance coverage dispute that we review in the next section.

III. *Merck & Co. v. Ace American Insurance Co.*[29]

A. Facts

On June 27, 2017, a world-wide dispersal of the "NotPetya" malware infected the computer system and 40,000 computers at Merck & Co. Inc. ("Merck"). Cost of the damage exceeded $1.4 billion. Merck had purchased $1.75 billion in property insurance from Ace American Insurance Company ("Ace") in the form of an "all risks" policy to secure it against loss or damage "resulting from destruction or corruption of computer data and software."[30]

Merck apparently filed a claim thereunder for the damage NotPetya caused to its computers. Ace apparently denied the claim, based on an exclusion in the policy for "warlike" actions. After filing suit against Ace in the Superior Court of New Jersey, Merck moved for partial summary judgment declaring that the "Hostile/Warlike Action" exclusion ("warlike action" exclusion) is inapplicable to the dispute. Ace cross-moved for summary judgment to declare the "warlike action" exclusion applicable. The court addressed the cross-motions for summary judgment.

B. Obsolescence of a Contract Language Paradigm

The "warlike action" exclusion clause at issue provided that the policy did **not** insure against:

> Loss or damage caused by *hostile or warlike action* in time of peace or war, including action in hindering, combating, or defending against an actual, impending, or expected attack: a) by any government or sovereign power . . . or by any authority maintaining or using military, naval or air forces . . .) or by an agent of such government, power, authority or forces.[31]

Ace argued that the exclusion language applied to damage caused by the NotPetya malware, which Ace characterized as "an instrument of the Russian Federation as part of its' [sic] ongoing hostilities against . . . Ukraine."[32] Ace argued that Merck's NotPetya losses thus came within the exclusion of damage "caused by hostile or warlike action" by a government power. Merck disputed that characterization and argued that even if NotPetya indeed originated from Russia's military action against Ukraine, the exclusion would still not apply.[33]

[29] No. UNN-L-002682-18, 2022 WL 951154 (N.J. Super. Ct. Jan. 13, 2022).

[30] *Id.* at *1.

[31] *Id.* at *1–2 (emphasis added).

[32] *Id.* at *1.

[33] *Id.*

Merck argued that it reasonably understood the “warlike action” exclusion language to refer solely to a government’s use of *armed forces* and that all existing case law on war exclusion supported its interpretation. The court found Merck’s argument persuasive and, in support, discussed cases that interpreted war exclusion language to refer to hostilities between the armed forces of two or more nation states. It noted that no court had applied a war or “warlike action” exclusion to “anything remotely close to the facts herein.”[34]

The court reached its decision without addressing the cyber “elephant in the room,” namely that for years Russia has utilized cyberattacks to inflict warlike harm, damage, and disruption. For example, there is the well-documented Russian cyberattack on Ukraine’s electric grid in December 2015, the first known cyberattack to have caused widespread blackouts; the attack included an irreversible overwriting of grid firmware, forcing operators of the affected sector of Ukraine’s grid to shift to manual operations for months thereafter.[35]

Cyberattacks present two levels of potential obsolescence of a security paradigm embedded in contract language (such as that contained in “warlike action” exclusion clauses): (i) the emergence of kinetic damage caused by state or state-sponsored cyberattacks as part of a belligerent state’s *non-traditional* arsenal of weaponry to strike, disrupt, and severely degrade an adversary state’s critical infrastructure; and (ii) the emergence of kinetic *collateral damage* in neutral countries caused by the spillover of the belligerent’s cyberattacks against an adversary state.

The court declared it “self-evident” that both parties were “aware that cyber attacks . . . sometimes from private sources and sometimes from nation-states have become more common.”[36] The court compared the growth in cyber risks to the “language used in these [“all risks”] policies [which] has been virtually the same for many years.”[37] The court thereby implied that both parties knew the security paradigm for “all risks” policies had shifted, putting commercial enterprises at increased risk of cyber attacks from private and state bad actors. Defendant insurer had the power to change the language of its “warlike action” exclusion clause to clarify its scope and signal that the language excluded damage caused by the emergent use by belligerent states of cyberattacks in “warlike” ways. As the court explained:

> Insurers did nothing to change the language of the exemption to reasonably put this insured on notice that it intended to exclude cyber attacks. Certainly they had the ability to do so. [Since insurers] failed to change the policy language, Merck had every right to anticipate that the exclusion applied only to traditional forms of warfare.[38]

[34] *Id.* at *6.

[35] Kim Zetter, *Inside The Cunning, Unprecedented Hack of Ukraine’s Power Grid*, WIRED (Mar. 3, 2016), https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[36] *Merck*, 2022 WL 951154, at *6.

[37] *Id.*

[38] *Id.*

Under New Jersey insurance law, the insurer has the burden of proof to show that a policy exclusion applies.[39] The applicable canon of construction is that "when the language used creates an ambiguity, the policy should be interpreted to conform to the reasonable expectations of the insured."[40] The insurer ignored the shift in the security paradigm brought about by the emergent use of cyberattacks by belligerent states. The insurer took the chance that the shift in the security paradigm would create circumstances in which it would be unclear whether the exclusion language applied to the new realities of enterprises experiencing collateral damage from a belligerent's use of cyberattacks. The insurer did not put the insured on notice that the unchanged language of the exclusion clause would be viewed by the insurer as changing its scope to exclude the emergent "warlike" use of cyberattacks. As a result, the court concluded: "Merck's position that they did not anticipate that the exclusion would be applied to acts of cyber based attacks reasonably shows that the expectation of the insured was that the exclusion applied only to traditional forms of warfare."[41]

The court decided in favor of Merck and granted Merck's motion for summary judgment that the "warlike action" exclusion clause did not cover the collateral damage caused to Merck's computers by the Russian Federation's release of Not-Petya worldwide.[42]

C. Digital Security Lessons

The *Merck* decision offers two security lessons. *First*, since drafters of contracts tend to reuse language that seems to have served them well in previous transactions, the habit of reusing language may create a complacency about the need to review and revise the language when security paradigms reflected in the language have shifted or changed. When nation states (or state-sponsored actors) make novel and malicious use of technological innovations, it often changes the existing threat and risk profiles and, in turn, renders obsolete the security paradigms embedded in contract language. At the first sign of such shifts or changes, counsel might consider recommending that clients review and update contracts whose language reflects the outdated security paradigms. Otherwise, the contract language may cease to reflect reality or to do so unambiguously. When that happens, it may be unclear whether the contract language applies to the emergent realities. Client and counter-party expectations about what the security-related language means might diverge, lead to misunderstandings, and provoke disputes. If the disputed language originated with the client and the client had the opportunity to update and clarify it, and did not do so, a court will

[39] *Id.* at *3.

[40] *Id.* at *2.

[41] *Id.* at *6.

[42] *Id.* Note that on February 24, 2022—the day Russian armed forces invaded Ukraine—the New Jersey Appellate Division granted Ace's motion for leave to appeal. James Vinocur, *What NotPetya Tells Us About Future Potential Cyber Risk Damages*, N.Y. L.J. (Apr. 21, 2022, 11:00 AM), https://www.law.com/newyorklawjournal/2022/04/21/what-notpetya-tells-us-about-future-potential-cyber-risk-damages/.

probably refuse to enforce the meaning the client wants and failed to revise the contract to express.[43]

Second, counsel should be wary of unexamined reliance on security terms that may seem precise, but whose meanings shift and become ambiguous when a security paradigm embedded in the words, or implied by them, abruptly changes. The *Merck* court, for example, did not have to address whether the exclusion clause applied only to damage caused by cyberattacks against a targeted enterprise, or whether it applied also to collateral damage against enterprises that were not targets of the cyberattack. The target vs. collateral damage distinction is crucial. It may arise within an attacked state (as between military and non-military targets). And it may arise in any state not directly targeted by the belligerent that released the malware. Counsel may find such clarification necessary not only in insurance contracts, but in any goods or service supply contract as well. Supply contracts typically involve issues such as *force majeure*, excusable delay, impracticable performance, and anticipatory breach. Those issues may turn on whether an alleged impediment to performance is covered by language that includes terms such as "war, "warlike," "cyberattack," "malicious use," or other terms that are linguistically *dual-use*—i.e., they may appear part of the "martial" or "military" lexicon, but also have non-military or collateral damage meanings whose application may be ambiguous. To avert such ambiguity, counsel and clients need to negotiate and clarify what they want the words to mean in the event of a cyber incident.

IV. Conclusion

The *Holbrook* and *Merck* cases each turned on a security tradeoff. In *Holbrook* the designer of the robot assembly line apparently decided on a tradeoff of human security in exchange for minimizing any interruption of robot operation for maintenance, repair, or malfunction correction. The *Holbrook* court seems to have discerned that tradeoff and would not grant summary judgment from product liability for the designer defendant. By not implementing that safeguard for human workers, the designer of the robot assembly line created a bias: if robot malfunction and human error combined, a human co-worker would likely be imperiled. Designers of robots and of robot/human working arrangements need to avoid putting humans in harm's way. To do that, they need to imagine ways that inevitable robot malfunctions and human errors may combine on the assembly line. They also need to consider that, if such harm can be averted (or reduced) by thoughtful programming, such harm can be triggered by sophisticated hackers. Security to safeguard humans must therefore be in both the design of the code

[43] Note that in November 2021, Lloyds Market Association (UK) "published four new cyber-warfare exclusions for use by underwriters" that curtail coverage for nation-state conducted "cyber operations." *Four New Cyber War Exclusions from Lloyd's Market Association*, Nat'l L. Rev. (Jan. 10, 2022), https://www.natlawreview.com/article/four-new-cyber-war-exclusions-lloyd-s-market-association.

and in the protection of the code from unauthorized access and malicious modification.

In *Merck*, the security tradeoff involved reuse of security language to avoid the need to revise it to keep pace with shifts in cyber and military security paradigms. Company executives see cost savings in adhering to company standard language for security-related clauses. Unfortunately, if counsel suggests the need to update such language to keep pace with shifts in a security paradigm, clients may think the need dubious and the cost obvious.

Clients may respond differently to such recommendations during Russia's war against Ukraine. The war has reportedly included multiple "cyber fronts" of conflict.[44] The security paradigms that prevailed before that invasion have changed utterly as reflected in the May 2022 decisions by unaligned states, namely Finland and Sweden, to seek admission to NATO.[45]

War tends to accelerate advances in technology and shifts and changes in security paradigms. Perhaps the outbreak of the increasingly large-scale, long-duration war in Eastern Europe will make clients and counsel more attentive to the need to adjust policies and security-related contract language, adapting it to the new contours of the rapidly changing security paradigms landscape.

[44] James Andrew Lewis, *Cyber War and Ukraine*, Center for Strategic & International Studies, Jun 16, 2022, https://www.csis.org/analysis/cyber-war-and-ukraine.

[45] *Finland and Sweden Submit Applications to Join NATO*, NATO (May 18, 2022, 9:08 AM), https://www.nato.int/cps/en/natohq/news_195468.htm.