Smart and Sustainable Manufacturing Systems

doi:10.1520/SSMS20210042 / Vol. 6 / No. 1 / 2022 / available online at www.astm.org

Praveen Sreeramagiri,[1] Gillian Andrews,[2] Amanda K. Greene,[3] and Ganesh Balasubramanian[4]

Analyzing Security Risks in Cyber-Physical Manufacturing Systems with Actor–Network Theory

Reference

P. Sreeramagiri, G. Andrews, A. K. Greene, and G. Balasubramanian, "Analyzing Security Risks in Cyber-Physical Manufacturing Systems with Actor–Network Theory," *Smart and Sustainable Manufacturing Systems* 6, no. 1 (2022): 110–121. https://doi.org/10.1520/SSMS20210042

ABSTRACT

This article suggests that actor–network theory (ANT) can reveal unique challenges and consequences of cyberattacks in manufacturing. As an approach, ANT rejects the dualism that often separates humans and nonhumans, recognizing the active role of both in affecting events. Our approach adds an important new perspective to an existing body of research that focuses on analyzing vulnerabilities in cyberspace instead of their ramifications in the material world. Drawing on the case study of a faulty airbag inflator in an automobile, we use concepts and vocabularies drawn from ANT to discuss the consequences of attacks in manufacturing, such as viewing altered products as actants with agency to alter subsequent networks (e.g., when a manufactured part is integrated into an automotive vehicle). By tracing the movement of specific materials and products through networks it is possible to elucidate how cyberattacks not only impact cyber-physical systems themselves, but also reverberate into a multitude of broader impacts, potentially endangering physical safety, shaping public opinion, and influencing economic markets. Our examination of one particular context draws on existing work that has brought ANT and cybersecurity in dialogue, but we extend this work by focusing on the role of "translation" and "depunctualization" across the lifecycle of a cyberattack in manufacturing. This analysis stresses the need for sector-specific examinations of cyberthreats, while also demonstrating the value of interdisciplinary methods like ANT that do not reify artificial dualisms in addressing for conceptualizing security risks in cyber-physical manufacturing systems.

Keywords

cybersecurity, cyber-physical systems, actor–network theory, manufacturing

Manuscript received October 15, 2021; accepted for publication April 4, 2022; published online May 12, 2022. Issue published May 12, 2022.

[1] Department of Mechanical Engineering and Mechanics, Lehigh University, 19 Memorial Dr. W, Bethlehem, PA 18015, USA

[2] Department of English, Lehigh University, 35 Sayre Dr., Bethlehem, PA 18015, USA

[3] Andrew W. Mellon Humanities Lab, Lehigh University, 27 Memorial Dr. West, Bethlehem, PA 18015, USA

[4] Department of Mechanical Engineering and Mechanics, Lehigh University, 19 Memorial Dr. W, Bethlehem, PA 18015, USA (Corresponding author), e-mail: bganesh@lehigh.edu, https://orcid.org/0000-0003-1834-5501

Cyberthreats in Manufacturing

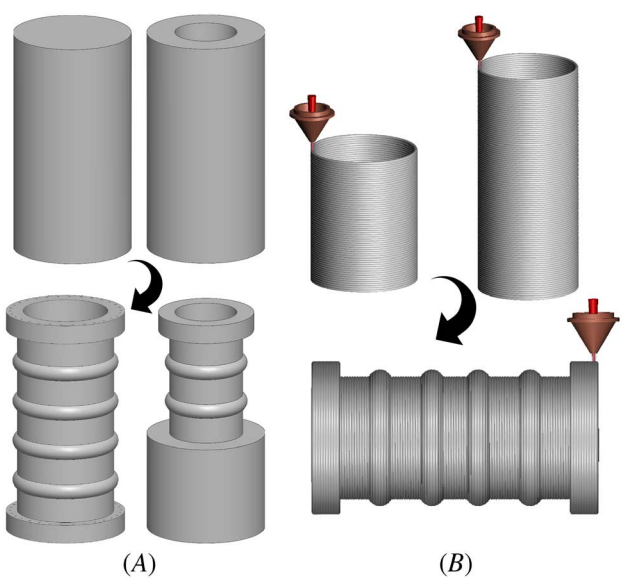
Recent developments in systems design coordinate both cyber and physical elements into complex networks. These cyber-physical systems (CPSs), which merge software and hardware to create new opportunities for remote control and automation, will likely increase in prevalence as smart technologies are integrated into households and industrial systems.[1] Although their dependence on cyber networks makes CPSs especially vulnerable to cyberattacks, these threats can be difficult to analyze and anticipate because of the intricate interdependencies between their physical levels (sensors that gather data and actuators that enact physical commands) and cyber levels (where the gathered data are stored and interpreted).[2] New investigations into the security of CPSs must focus on its unique challenges,[3,4] distinct from traditional IT (information technology) security.[5]

Cybersecurity vulnerabilities pose problems for all CPSs, however the manufacturing sector has a unique set of security concerns. Here we focus on machining (a.k.a., subtractive manufacturing) and additive manufacturing (AM) techniques, as they are prone to a higher risk compared to others. The processes are illustrated in **figure 1**. Both techniques use computer-controlled machines (CPSs) and human technicians (labor) to produce the final product. In both cases, the design starts from a computer aided design model (a virtual part created in a computer) that is then fed to another software (pre-processor) to generate a tool path based on the features of the component. Both processes require the same steps, except that machining works by removing material and AM adds the material layer by layer. The evolution of these processes to be predominantly digital readily invites cyberattacks,[6] and their direct association with the physical product potentially impacts other systems and users outside the original CPS.

Cyberattacks in manufacturing are complex phenomena with wide-ranging consequences. Loukas, for example, identifies five kinds of cascading physical outcomes that can stem from a cyberattack: breach of physical privacy, unauthorized actuation, incorrect actuation, delayed actuation (false data injections), and prevented actuation (denial of service attacks).[7–10] While each of these can occur in a manufacturing CPS, the latter three are of most urgent and specific concern to this sector. To offer a concrete example, incorrect actuation and prevented actuation were consequences of a cyberattack at a Honda factory in 2017. WannaCry ransomware infected production line computers in the plant, shutting these computers down (prevented actuation) and causing approximately 1,000 units to be faulty (incorrect actuation). Subsequently, the entire plant was forced to shut down for a

FIG. 1

Two approaches to manufacture the same component.
(*A*) Machining: A part is manufactured by the removal of material from a cast or wrought ingot; (*B*) Additive Manufacturing: A part being fabricated by the addition of material, typically layer by layer, until the part is completed. The same part being manufactured in steps by adding material.



day (further prevented actuation).[11] Other attacks can include intent to steal proprietary design files to print parts elsewhere[6] or to directly sabotage or alter the design of products being manufactured. The alteration of a design (incorrect actuation) is most concerning in the manufacturing sector as it can compromise the integrity of parts and potentially have disastrous impacts. These harms can be both economic (for companies) and pose potential danger to human life.[12]

We propose an interdisciplinary approach, viz., actor–network theory (ANT), which can serve as a tool to complement established threat mitigation measures by industries (such as machine learning models to predict potential attacks) by elucidating the sociotechnical nature of the problem. While initial threat mitigation research primarily relies on quantitative methods like risk analysis or machine learning in response to CPS security,[7,13,14] ANT can address specific needs of the manufacturing sector by articulating complex modes of human-object entanglement with meticulous material specificity. In this article we first offer a brief overview of ANT and the core vocabulary we believe is most useful in the case of manufacturing CPSs. We then build on previous scholarship theorizing ANT in relation to cybersecurity problems in order to develop new conceptual models rooted specifically in the manufacturing sector that highlight material specificity and the work of translation. We conclude by applying these concepts to the concrete case study of a faulty airbag in an automobile. This sector demands such interdisciplinary approaches because an attack is not limited to cyberspace; a manufacturing CPS produces physical products that may have serious consequences elsewhere. By examining the networks these products move through, ANT can help uncover the socioeconomic impacts of cyberattacks that are often overlooked and illuminate the importance of attending to the material specificity of attacks in this sector.

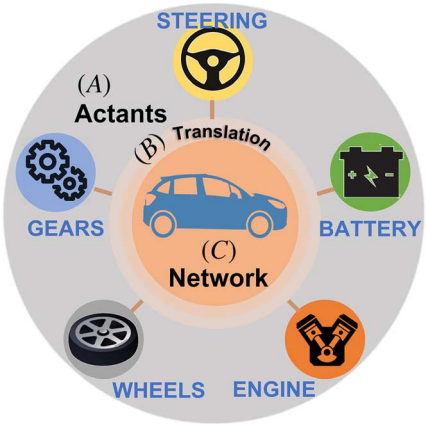
Our intervention helps extend the growing body of literature that brings science and technology studies (STS) to bear on cybersecurity as well as introducing ANT into the increasingly vital domain of manufacturing CPSs. While ANT has increasingly become part of cybersecurity conversations, it has yet to be applied to the specific context of cyber-physical manufacturing systems. Through this application, our efforts offer a new vantage on threat mitigation in manufacturing while also refining the application of ANT in this context. Specifically, ANT concepts like translation provide a lens to consider the cultural and socioeconomic meaning-making that stems from cyberattacks as distinct from, but still connected to, any immediate material damage. Such methods can prove crucial understanding within the broader consequences of cyberattacks, enabling quantitative derivation of weights geared toward consequence informed prediction of cyberattacks; directed toward making informed policymaking decisions for any industry to mitigate such attacks.

ANT Core Concepts

ANT is a paradigm thinking about the world that has emerged from STS and sociological approaches to understanding technological innovation in society.[15–18] ANT views both human and nonhuman entities as possessing agency; it thereby rejects the binary opposition often assumed between "social" and "technological" worlds, stressing instead that these realms are inseparably entangled and coproduce with one another.[19] The theory therefore foregrounds the relationships between humans and nonhumans, as well as the way these connections dynamically influence and construct the world. An overview of the ANT is presented in **figure 2**. Next, we briefly introduce several pertinent terms coined by ANT scholars (actants, actor–networks, depunctualization, and translation) and extend these descriptions to highlight their importance to cybersecurity in manufacturing.

ANT introduces the concept of actants to reform the way we think about relationships between humans and nonhumans. Actants indicate the possession of agency and can describe both human and nonhuman entities. Whether discussing the role of a person, a computer, or a simple object, any entity can be considered an actant as long as it is the source of an action.[20] Rather than viewing objects as passive "things," ANT adopts a principle of generalized symmetry that considers both humans and nonhumans to be capable of shaping the world around them.[19] The term actants provides language for the equal analysis of the roles that social and technical entities play in co-constructing society and technologies.

FIG. 2 An illustrative representation of actor-network theory based on the automotive manufacturing industry; (*A*) Gray shaded area constitutes multiple actants that influence the process of a network; (*B*) The transition from gray to orange represents the process of translation, where the actants are being engaged into the network; and (*C*) constitutes a network that is the product of all the actants and translation.



Within an ANT framework, actants are arranged to constitute actor–networks. These networks are entities that might appear to be one cohesive unit from one vantage but are made up of many actants working together to produce a functioning system. For instance, we might consider an infrastructure that produces turbine blades for airplanes. While it would not be incorrect to call this unified location and single entity a "factory," it is also a network of actants working together. What we often think of as a single factory is a complex set of interconnected actants that span human workers, software design programs, computer hardware, 3D printers, conveyer belts, computer code, human coders, malleable plastics or metals, and more.

The term actor–network recognizes the complex relationship between an actant and a network: "An actor–network is simultaneously an actor whose activity is networking heterogeneous elements and a network that is able to redefine and transform what it is made of."[21] In the context of an entire factory, a computer can be understood as an actant, but that computer is itself also a network of smaller parts and software. The scope of analysis often determines what is analyzed as an actor–network and what is accepted as an actant. Hence, it is important to realize that for any CPS, there can exist a hierarchical classification of actors and networks. The appropriate scale for selecting actors versus networks in any given case is necessarily rooted to the problem of interest and must be carefully considered.

The way we perceive networks and actants is influenced by the third core ANT concept: punctualization (and its complement depunctualization).[22] As noted in the examples of a factory or a computer, we often do not see the complexity of the human-nonhuman interrelationships that make up the actor–networks around us; the successful operation and fulfillment of duties by networks overlook the necessity to think of them as collections of parts. Punctualization is this act of a network being rendered invisible by its successful operation. Take Restivo's explanation of the concept that uses a car as an example. When everything in the car-network is in working order, we simply see a car, meaning that the network is punctualized. However, when the car breaks down, we are prompted to view it as a collection of individual parts in order to find the source of the problem. This depunctualization (see **fig. 3**) is the moment when we see a supposedly cohesive object (when all parts of the network are functioning as intended) as a collection of parts (when the network breaks down, rendering it visible).[23]

The final ANT construct we use here is translation. Translation is the process by which individual actants become enrolled in an actor–network and how the actor–network attains a collective project or identity. It is the process of bridging the gaps between all the actors that are combined in the network. To make this possible,

FIG. 3 (*A*) Punctualization: A car, as a whole, is viewed as a network when it is working perfectly; (*B*) Depunctualization: Realization that the network (car) is a collection of different actants (components) to determine and fix the issue of the network in an event of a problem (car break-down). Depunctualization is not a physical act/change but essentially a shift in perception of the user seeing the car as composed of many different parts all working together, rather than one cohesive unit.

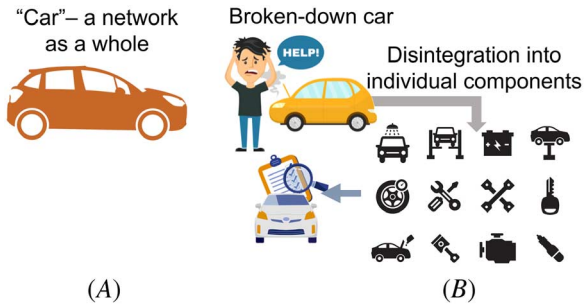
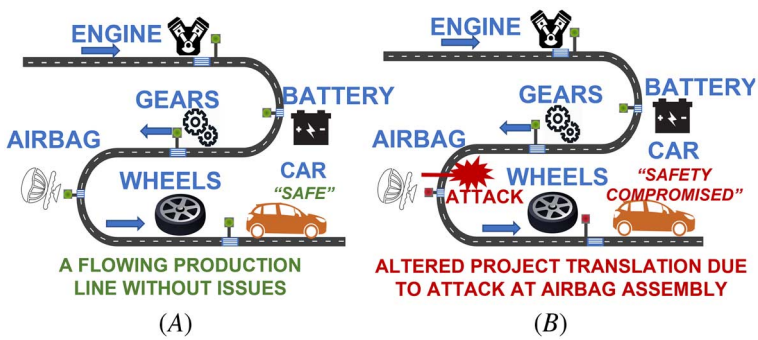


FIG. 4 Pictorial reproductions of functioning versus attacked network. (*A*) Functioning network: all the actants in the network are operating and performing as they are meant to be; and (*B*) Attacked network: When an actant of a network is attacked, it may lead to several consequences including, but not limited to, alteration of parts, human life endangerment, etc. An attack on the airbag when left unnoticed can compromise the safety of the car, result in a catastrophe when in use, and lead to a change in translation of the project.



a translator adopts the responsibility of assigning an actant a particular role to give it a purpose.[24] At this stage, the translator (a company with a stake in the network, for example) acts as a spokesperson of the network to create an environment where it can function hassle-free. In the aforementioned example of a factory producing airplane turbines, the company that intends to profit and gain a reputation for safe and reliable turbine manufacture translates the actants in the factory into an infrastructure that can achieve those social goals for the company. In other words, the translator strategically enrolls the actants to work together as a coherent network.[25] Notably, translation is always an ongoing process and can be interrupted or contested by alternate interpretations and events, such as cyberattacks.

Cybersecurity and ANT

To the knowledge of the authors, as of this publication no existing research has explored how ANT can intervene in understandings of security in cyber-physical manufacturing systems. Still, in making this novel turn, we build rigorous precedents in the fields of human–computer interaction and cybersecurity. The consistency with which ANT has been applied to evolving issues in cyberspace demonstrates that its core tenants are applicable to many

facets of human–computer relationships and the protection of users. As the complexity of human relationships with computers has evolved, scholarship has begun to turn to ANT as an analytical tool that can grapple with these entangled encounters. ANT was praised as early as 1999 by Tatnall and Gilding for avoiding the essentialist binary oppositions inherent in other extant methods of analysis like ethnography, instead enabling IT research where "interactions of the social, technological, and political are regarded as particularly important."[26] ANT was subsequently used to think about emerging issues in cybercrime, with a review of articles by Luppicini indicating promising results.[27]

A small body of research has also directly mobilized ANT in the context of cybersecurity. For example, Stachel and DeLaHaye use ANT principles to discuss risk mitigation for breaches in healthcare data security and Pieters utilizes ANT to propose new methods of integrating human behavior into systems modeling.[28,29] Crucially, Balzaq and Cavelty have shown how ANT can help look beyond problem-solving models which focus narrowly on identifying vulnerabilities and instead advocate for analysis that expands beyond cyberspace and the initial moment of attack.[30] In their analysis of Stuxnet malware, Balzaq and Cavelty argue that ANT can help us consider the political consequences and contexts of cyberattacks. The very recent work of Liebetrau and Christensen, which brings ANT to bear on cyber-physical entanglements through their focus on the ontological politics of the Internet of Things (IoT) and the Mirai botnet, is also an essential intervention that we build on. Their work emphasizes the importance of understanding cyber insecurities as emerging from "collective, performative, and relational processes" across a multiplicity of domains as opposed to individualized actions.[31,32]

Cyber-Enabled Manufacturing as a Proving Ground

We suggest that the complexities of attacks on manufacturing CPSs can only be understood through expanded attention to material specificity, to the movement of physical products through multiple networks, and to the subsequent socioeconomic consequences of their movement. Balzaq and Cavelty's ANT-informed definition of cyberattacks is our starting point: "cyber-incidents are depunctualizations of cybersecurity networks by mediators in the form of malware, with effects in regional, networked, and fluid spaces."[30] However, we also complicate their definition by asserting that in the context of manufacturing, the concept of translation cannot be neglected and is just as crucial as depunctualization in terms of identifying vulnerabilities and mitigating threats.

Cyber-physical attacks in manufacturing have consequences that span multiple networks and operate on socioeconomic levels as well as cyber and material levels. In the case of a complete shutdown (prevented actuation), for instance, the absence of available products will impact the productivity of the factory-network itself first. Subsequently, in a moment of depunctualization, the component actants of the factory and its security come under scrutiny to find the source of the problem, whether it be a careless worker who fell for a phishing scam, or, in the case of the Honda WannaCry attack, outdated computers. This depunctualization also compromises the confidence in the competency of the manufacturer and potentially affects the profit margin of the parent company (another network in its own right). If those products being manufactured are parts that would then be integrated into other components (e.g., an airbag casing that would be put into a car), the temporary absence of new stock could influence other factory-networks that need them to fabricate their products. If the company is deemed careless under public scrutiny for not preventing the attack, the incident could affect public opinion and even stock prices.

These multinetwork and social consequences occur in various kinds of cyber-physical attacks in manufacturing. The greatest risk is associated when the defective or altered products go undetected and are integrated in the other networks. We place our focus here given that these knock-on effects on other networks have the highest potential for harm. In this case, defective or altered actants produced by the initial factory-network run the risk of being integrated into other networks if the fault is undetected. These sprawling impacts are never more clearly seen than in the case of cyberattacks that aim to alter products themselves (incorrect actuation).

While it might be assumed that products altered by cyberattacks would be easily identified and discarded, there is actually significant potential for these errors to go unnoticed. Some defects embedded within a 3D printed product

have been discovered by Zeltmann et al.[33] to be undetectable by ultrasonic inspection and could potentially compromise the strength of the final product. Such defects can result from command alterations (a consequence of false data injection) as simple as changing the printing direction, which can easily go unnoticed during inspection. Similarly, Ranabhat et al. simulated optimal sabotage attacks on the production of a load-bearing element of an airplane wing, concluding that attacks on the material's orientation during production would create deficiencies in specific material properties that are difficult to detect during product testing.[34] In each of these cases, defects have the potential to remain concealed until the moment in which they endanger users.

Furthermore, several experiments have shown that humans can fail to identify defective parts resulting from unknown cyberattacks. Wells at al. found that students had difficulty identifying parts altered to the degree that, were they put into use, "the end product would prematurely or catastrophically fail in-use." Even when the flaw was identified none of the students could link the altered product to an instigating cyberattack.[35] A similar experiment by Strum et al. also found students were often incapable of identifying defective products, even when they tested them.[36] These studies demonstrate that confidence in automated systems and a lack of awareness regarding the possibility of an undetected cyberattack can cause human error and inhibit the rapid identification of defective parts. While data about real incidents of unnoticed defective parts due to cyberattacks are scarce and would be unlikely to be disclosed to the public unless a catastrophic accident occurs, analyzing the potential consequences of such an attack is warranted because of the proven potential for such an oversight to occur (see the 2019 literature review from Elhabashy, Wells, and Camelio for a more comprehensive summary.[37])

In tandem with these technosocial concerns, material specificity (or the attention to the unique agencies of the particular nonhuman nodes in the network) is another important feature while analyzing cyberattacks in manufacturing using ANT. Thus far, we have largely discussed the potential consequences of cyberattacks in relation to nebulous "products" that have not been specified in order to provide a generalized overview of issues in manufacturing cybersecurity. Materials, however, are not interchangeable, nor are the roles that different products play in their respective networks. For instance, analyzing the impact of an attack that compromises the integrity of core components of a car is different from analyzing an attack which altered the quality of components that are installed for increased luxury (even if the two attacks were conducted by the same attacker with the same malware, exploiting the same security vulnerabilities). In order to fully explore the consequences of a product altering cyberattack in the manufacturing sector, we must discuss case studies which utilize particular materials, products, and networks.

Case Study: Faulty Airbag Inflators

We turn to automobile manufacturing as a case study for several reasons, including a lack of reliable data on the motivations and resources for cyberattacks. On the one hand, cars have been used as illustrative network models in earlier ANT studies (like Restivo's explanation of punctualization[23] and Callon's famous analysis of an early electric car[24]), which enables a concrete connection between ANT scholarship and this application. On the other hand, we benefit from the availability of reports (Honda's 2017 factory shutdown due to WannaCry ransomware[11]) and public knowledge on the impact of cyberattacks on car manufacturing networks—information that remains elusive in many other sectors. Additionally, the ramifications of manufacturing defects in car parts are well documented through statistics about vehicle recalls and case studies about car part safety. While most defects are caused by accidents, human error, or design flaws, rather than deliberate cyberattacks to alter the part, the literature surrounding car part imperfections provides important grounding in extrapolating the potential effects of a defect caused by a deliberate attack. As Morris, Madzudzo, and Garcia-Perez have noted,[38] the auto industry's reliance on integrating many different components gathered from geographically disparate suppliers can open the industry to cybersecurity attacks at a number of levels. This vulnerability is because "current integration strategies were developed before the ubiquitous implications of automotive cybersecurity threats were appreciated and, as a result, most component integration strategies are not cyber-resilient."[38] Thus, the automotive manufacturing industry offers a current and compelling case study for an ANT approach to CPS cybersecurity.

AIRBAGS–AN INTRODUCTION

Airbag inflators are components integrated into automotive airbag safety modules in order to quickly inflate the airbag with gas in the event of a collision. This reduces the impact received by the drivers, passengers, or both, to prevent injuries during a crash. Airbags function on the basis of multiple chemical reactions that promote the inflation of the bag in less than a second. The inflator of an airbag consists of three solid chemicals, sodium azide, potassium nitrate, and silicon dioxide, which are decomposed to nitrogen gas and nontoxic alkaline glass when the reaction is initiated (in a span of ~40 ms). Manufacturing flaws (e.g., in the strength of the casing that contains the chemicals) in the cannister enclosing the chemicals can result in penetrating injury and even death.[39] As a component that affects human safety in catastrophic moments, the consequences surrounding an altered airbag inflator, as an example, allows a clear understanding of the stakes involved.

A HYPOTHETICAL CYBERATTACK (ANT PERSPECTIVE)

From an ANT perspective, an airbag inflator manufacturing facility is an actor–network of many actants working together to produce a desired effect; in this case, the production of a safe and functional part for an auto component. A cyberattack into this system with the intent of altering the design of an inflator would breach system security to disrupt the functioning of one or more actants. If detected, the mitigation process could involve discarding the produced inflators that are identified as defective during quality control. During a more insidious attack seeking to cause long-term damage via compromised parts that pass quality control measures, the attacker would need to remain undetected in order to prevent additional scrutiny of products.

Defects in airbags and inflators are well documented, making up some of the most ubiquitous auto defects in recent memory. Takata air bags, for instance, have faced waves of recalls as recently as 2019 because of the possibility of them spraying metal pieces while being inflated in the moment of collision. This defect has affected approximately 63 million air bags.[40] In a previous study,[39] the authors analyzed an accident where an unspecified brand of airbag killed a 22-year-old driver. In this incident, a faulty seal on the airbag inflator caused the booster cannister of cylinder to separate and the metal fragments in the component to shatter, launching metal shrapnel through the airbag and killing the driver.[39] While not caused by a cyberattack, this example demonstrates the risk a defective airbag inflator can pose to human life.

In the case of an airbag inflator, an undetected attack on the principal factory-network that altered the inflators' material integrity would have ramifications on other networks. Just as the factory is an actor–network of human and nonhuman actants, so too is a car. It is a complex entanglement of seats, carburetors, headlights, pedals, an engine, lights, in-car computer systems, hardware and software, gas in the gas tank, a key, a human operator, and hundreds of other actants. Each component is vital to the project of creating a safe and functional car that fulfills its purpose to transport people. In the case of a compromised airbag inflator, it is assumed to be a functional aspect of the car-network unless it is utilized, i.e., in the event of collision, which is when it is revealed as defective.

ANT ANALYSIS

We begin analyzing this scenario with the basic definition from Balzaq and Cavelty that "cyber-incidents are depunctualizations of cybersecurity networks by mediators in the form of malware, that effects in regional, networked, and fluid spaces."[30] By this definition, a cyberattack makes all the components of a network visible when their end-goal is disrupted and their functioning must be examined. The scenario of an altered (or compromised) part already requires additions to this definition. Depunctualization is a consequence caused by the disruptive perception of an attack; so if an attack remains undetected, this moment of depunctualization is deferred until it is found. We must therefore recognize the temporal flexibility of this depunctualization.

Likewise, in manufacturing, a single moment of depunctualization in the factory-network is not all that occurs. When the faulty airbag inflator is identified in a car, there is also a secondary moment of depunctualization in the car-network. Subsequent networks are also impacted by depunctualizations stemming from the initial intrusion. This multilevel aspect highlights that the temporality of depunctualization is not static. Here,

depunctualization may occur first in a secondary network (car) affected by the defective part, rather than in the primary factory-network. Only subsequently might the initial cyberattack be identified as the cause of the part failure, and then depunctualization of the factory-network would occur. This realization is now potentially far removed from the time of the initial cyberattack. How are we to conceptualize the complexity of a cyber-physical attack, if seeing it as an immediate moment of depunctualization in security networks is not flexible enough?

Incorporating the notion of translation into an ANT definition of cyber-physical attacks can help us look beyond the initial moment of intrusion. In manufacturing cars, the parent company enrolls many actants in the project of making a car that will be perceived as safe, desirable, and functional in order to generate company profits. Only when enrolled into this project by the translator-spokesperson (company) do the individual actants cohere together and actor–networks come into being. However, as Callon highlights, translation is always an ongoing practice rather than something that can be finally achieved; it can always be contested.[24] By attacking a factory-network and altering an airbag inflator to sabotage the eventual functioning of a car, an attacker is also altering the eventual message (e.g., reputation) rendered by the factory-network. While typically it is not possible to comprehend the exact intent of a potential attacker, it is possible to trace the potential consequences of alterations to understand the impacts of contested translation.

CONSEQUENCES OF THE CYBERATTACK

In this scenario, we recognize a sprawling set of connections forming: An initial cyber intrusion alters the airbag inflator, which is undetected in quality control. This part then malfunctions in a subsequent car-network, depunctualizing the car-network and revealing its component actants, and potentially causing significant harm to human users. If this fault is traced back to the original cyberattack, the factory-network will also be depunctualized by the intrusion. Depunctualization, as a consequence of the cyberattack, can damage multiple company networks. Because of this damage enacted across multiple networks, the cyberattacker has temporarily hijacked the role of translator-spokesperson for the factory and company networks. This hijack causes the factory and company networks to produce harmful products and associations rather than successful and reassuring ones. Thus, cyber intrusion potentially promotes economic consequences, including damage of their reputation for the company network as a whole.

Viewing cyberattacks as a single moment of depunctualization does not account for the complexity of this multinetwork consequence because of the physical circulation of the manufactured parts. The case of the airbag inflator establishes the danger of a contested translation that compromises one aspect (the airbag) of the company reputation for safety. As drivers only use airbags in rare moments of extreme danger, their role in the car-network is complex. They do, of course, serve the eventual purpose of protecting drivers in a collision if all components are functioning as they should, but beyond this they serve a role in the car-network every day to create trust in the user. If trust cannot be placed in a particular brand of airbag or car because of a spate of dangerous defects, users may not wish to enroll the car-network that is now not trusted as "safe." Damage to the reputation of a company via engineered airbag defects could have consequences for car-networks that do not even possess that defect if public fear were to be stoked enough. The cyberattacker would have successfully sabotaged the company translator-spokesperson's project and altered the meaning communicated by the factory, car, and company networks. Such altered translations from "safe" to "unsafe," "responsible" to "irresponsible," could harm company profits, stocks, and subsequently result in the loss of reputation.

By attacking a factory-network and altering an airbag inflator to disrupt the eventual functioning of a car, an attacker is therefore also altering the eventual message (e.g., reputation) produced by the factory-network. If the part creates a dangerous or suboptimal car, no longer is the factory-network successfully enacting the role assigned by the company translator-spokesperson. Rather than the network creating products that connote safety, desirability, and convenience for the company and end user, the cyberattacker has taken on a spokesperson role contesting the original translation intended by the company; they are translating the network for a new project. This project could be intended to achieve several things: to impact stock prices, reduce company's profits, cause harm to human users rather than enact safety, etc. In other cases—for example, an impaired, noisy muffler being integrated into

a car-network—the loss of human life would not be a likely consequence. Instead, issues of company reputation and user choice would be influenced by altered user experience and public perception. Decisively, translation of a network can be disrupted by an attacker even if that is not the initial intention. Even malware that is unintentionally released into a network (or released for other reasons) can alter the meanings connoted by that network via impacts on safety and reputation, as seen in the case of the airbag inflator. The cultural and socioeconomic consequences of this retranslation therefore still occur, even if they were not the primary intent, and must still be considered.

While depunctualization remains an important aspect, translation provides an additional lens for conceptualizing the complexity of cyber-physical security attacks. We thus suggest an augmented version of Balzaq and Cavelty's definition to express the impact of attacks on manufacturing CPSs: "Cyber incidents in manufacturing are depunctualizations of cybersecurity networks by mediators in the form of malware, which, if successful, can cause further depunctualizations in subsequent networks and retranslate the project of the network, thus having both physical and socioeconomic consequences."

This definition requires an approach that recognizes the material specificity of an altered part and an understanding that no two parts will influence subsequent networks in the same way. Armed with this expanded definition, cybersecurity researchers in manufacturing can use ANT concepts to consider the outcomes of attacks on networks at multiple levels: the primary factory-network; subsequent networks the component is integrated into, like a car-network; and even the large-scale company network and its functioning.

Summary

Expanding discussions of cybersecurity beyond initial moments of intrusion and carefully attending to the material specificity of involved parts is vital to addressing the complexity of this issue in the manufacturing sector. Where researchers in cybersecurity focus primarily on identifying vulnerabilities, an ANT approach demonstrates the need to consider factors both after (the multinetwork consequences) and also before this moment (the intent of the attack might impact the translation enacted upon the network by the intrusion). The application of humanistic social theory like ANT to technical engineering and manufacturing issues opens new possibilities for analysis. Together these fields can address both the technical and social complexities of cyberthreats in manufacturing with more nuance and a broader scope then either would be likely to achieve alone. Concretely, an ANT-informed perspective on cybersecurity breaches better accounts for their complexity in the manufacturing sector. Addressing specific vulnerabilities remains vital, but recognizing networked consequences can enhance our understanding of attacks. As CPSs continue to rise in popularity and cyberthreats evolve, new ways of conceptualizing the complexity of our entanglements with technology are vital.

The importance of merging ANT approaches to cybersecurity with manufacturing research leads to important conclusions for both fields. By reading the consequences of attacks in terms of networks and the creation of meaning, ANT illustrates the many kinds of harm that can stem from cyberattacks in this sector and how they are interlinked. This theory emphasizes the importance of enhanced quality control measures to prevent sprawling harmful consequences from overlooked abnormalities in parts. The focus on social reputation and its socioeconomic impacts highlighted by this approach can help demonstrate to profit-driven companies that investing in further cybersecurity and quality control is important to securing long-term economic success as well as user safety. Furthermore, our approach underscores the need for material specificity in addressing these concerns. While a particular kind of cyberattack could exploit the same vulnerability in a number of different factories, the particular consequence of the attack (especially if product sabotage is the goal) will change depending upon the specific materials affected. This outcome will determine the networks impacted by the attack, and therefore the kinds of protections and checks needed to fully protect the multiple networks from attacks. Presently, no analysis that discusses a nebulous or interchangeable "product" affected by a cyberattack can consider this complexity.

In the case of broader ANT-driven cybersecurity research, applying these approaches to manufacturing illuminates how cyberattacks can have sprawling physical, as well as social, consequences. Manufacturing is

an especially fruitful ground to explore the ways in which ANT concepts can aid our understanding of cyberattack impacts and can complement the growth of work focused on the IoT. Furthermore, considering the role of translation in cyberattacks is one method that can expand conversations about how cyberattacks influence networks in multiple ways. Considering the importance of connotation, social opinion, and broader meaning creation caused by cyberattacks also highlights the potential for interdisciplinary input when responding to attacks, where attention from scholars from fields like media studies, communications, and STS could offer valuable insight into understanding and mitigating social consequences. We have shown that cyberattackers do not simply make networks visible to analysis via depunctualization—although this does happen when attacks are perceived—but they actively create and alter meanings as translators.

ACKNOWLEDGMENTS

This material is based on the work supported by an interdisciplinary research grant from the Andrew W. Mellon Humanities Lab at Lehigh University, and in part by the National Science Foundation (NSF) through the award no. 1944040. We acknowledge the encouragement from Prof. Michael Kramp at Lehigh University to pursue this research.

References

1. S. K. Khaitan and J. D. McCalley, "Design Techniques and Applications of Cyberphysical Systems: A Survey," *IEEE Systems Journal* 9, no. 2 (June 2015): 350–365, https://doi.org/10.1109/JSYST.2014.2322503
2. R. Vigo, "The Cyber-Physical Attacker," in *SAFECOMP 2012: Computer Safety, Reliability, and Security* (Berlin/Heidelberg, Germany: Springer-Verlag, 2012), 347–356, https://doi.org/10.1007/978-3-642-33675-1_31
3. M. Anand, E. Cronin, M. Sherr, M. Blaze, Z. Ives, and I. Lee, "Security Challenges in Next Generation Cyber Physical Systems," in *Beyond SCADA: Networked Embedded Control for Cyber Physical Systems* (Pittsburgh, PA: Cyber-Physical Systems Virtual Organization, 2006), 1–4.
4. A. A. Cárdenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sastry, "Challenges for Securing Cyber Physical Systems" (paper presentation, Workshop on Future Directions in Cyber-Physical Systems Security, Newark, NJ, July 22–24, 2009).
5. A. Zarreh, H. Wan, Y. Lee, C. Saygin, and R. A. Janahi, "Cybersecurity Concerns for Total Productive Maintenance in Smart Manufacturing Systems," in *29th International Conference on Flexible Automation and Intelligent Manufacturing (FAIM 2019)* (Amsterdam, the Netherlands: Elsevier, 2019), 532–539, https://doi.org/10.1016/j.promfg.2020.01.067
6. F. Chen, G. Mac, and N. Gupta, "Security Features Embedded in Computer Aided Design (CAD) Solid Models for Additive Manufacturing," *Materials & Design* 128 (August 2017): 182–194, https://doi.org/10.1016/j.matdes.2017.04.078
7. F. Di Maio, R. Mascherona, and E. Zio, "Risk Analysis of Cyber-Physical Systems by GTST-MLD," *IEEE Systems Journal* 14, no. 1 (March 2020): 1333–1340, https://doi.org/10.1109/JSYST.2019.2928046
8. Q. Liu, T. Liu, Z. Liu, Y. Wang, Y. Jin, and W. Wen, "Security Analysis and Enhancement of Model Compressed Deep Learning Systems under Adversarial Attacks," in *23rd Asia and South Pacific Design Automation Conference (ASP-DAC)* (Piscataway, NJ: Institute of Electrical and Electronics Engineers, 2018), 721–726, https://doi.org/10.1109/ASPDAC.2018.8297407
9. M. Ahmed, A. N. Mahmood, and J. Hu, "A Survey of Network Anomaly Detection Techniques," *Journal of Network and Computer Applications* 60 (January 2016): 19–31, https://doi.org/10.1016/J.JNCA.2015.11.016
10. G. Loukas, *Cyber-Physical Attacks: A Growing Invisible Threat*, 1st ed. (Oxford, UK: Butterworth-Heinemann, 2015).
11. P. Lyon, "Cyber Attack at Honda Stops Production after WannaCry Worm Strikes," *Forbes*, June 22, 2017, https://perma.cc/343Q-T4LQ
12. M. Wu and Y. B. Moon, "Taxonomy of Cross-Domain Attacks on CyberManufacturing System," in *Complex Adaptive Systems Conference with Theme: Engineering Cyber Physical Systems* (Amsterdam, the Netherlands: Elsevier, 2017), 367–374, https://doi.org/10.1016/j.procs.2017.09.050
13. M. Wu, Z. Song, and Y. B. Moon, "Detecting Cyber-Physical Attacks in CyberManufacturing Systems with Machine Learning Methods," *Journal of Intelligent Manufacturing* 30, no. 3 (March 2019): 1111–1123, https://doi.org/10.1007/s10845-017-1315-5
14. D. Gao, Q. Huang, G. L. Zhang, X. Yin, B. Li, U. Schlichtmann, and C. Zhuo, "Bayesian Inference Based Robust Computing on Memristor Crossbar," in *58th ACM/IEEE Design Automation Conference (DAC)* (Piscataway, NJ: Institute of Electrical and Electronics Engineers, 2021), 121–126, https://doi.org/10.1109/DAC18074.2021.9586160
15. M. Callon and B. Latour, "Unscrewing the Big Leviathan: How Actors Macro-Structure Reality and How Sociologists Help Them to Do So," in *Advances in Social Theory and Methodology*, ed. K. K. Cetina and A. V. Cicourel (Boston, MA: Routledge & Kegan Paul, 1981), 277–303.
16. B. Latour, *Reassembling the Social: An Introduction to the Actor-Network-Theory*, 1st ed. (Oxford, UK: Oxford University Press, 2005).

17. J. Law, "Actor Network Theory and Material Semiotics," in *The New Blackwell Companion to Social Theory*, ed. B. S. Turner (Hoboken, NJ: Wiley-Blackwell, 2009), 141–158, https://doi.org/10.1002/9781444304992.ch7
18. M. D. Cavelty, "Cybersecurity Research Meets Science and Technology Studies," *Politics and Governance* 6, no. 2 (June 2018): 22–30, https://doi.org/10.17645/pag.v6i2.1385
19. J. Bennett, *Vibrant Matter: A Political Ecology of Things* (Durham, NC: Duke University Press, 2013), https://doi.org/10.1215/9780822391623
20. B. Latour, "On Actor-Network Theory: A Few Clarifications," *Soziale Welt* 47, no. 4 (1996): 369–381.
21. M. Callon, "Society in the Making: The Study of Technology as a Tool for Sociological Analysis," in *The Social Construction of Technological Systems: New Directions in the Sociological and History of Technology*, ed. W. Bijker, T. Hughes, and T. Pinchi (Cambridge, MA: MIT Press, 1987), 83–103.
22. J. Law, "Notes on the Theory of the Actor-Network: Ordering, Strategy and Heterogeneity," *Systems Practice* 5, no. 4 (August 1992): 379–393, https://doi.org/10.1007/BF01059830
23. S. Resvito, "Bruno Latour," in *The Wiley-Blackwell Companion to Major Social Theorists*, ed. G. Ritzer and J. Stepnisky (Oxford, UK: Blackwell Publishing, 2011), 520–540, https://doi.org/10.1002/9781444396621
24. M. Callon, "The Sociology of an Actor-Network: The Case of the Electric Vehicle," in *Mapping the Dynamics of Science and Technology*, ed. M. Callon, J. Law, and A. Rip (London: Palgrave Macmillan, 1986), 19–34, https://doi.org/10.1007/978-1-349-07408-2_2
25. M. Callon, "Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay," *The Sociological Review* 32, no. 1 (May 1984): 196–233, https://doi.org/10.1111/j.1467-954X.1984.tb00113.x
26. A. Tatnall and A. Gilding, "Actor-Network Theory and Information Systems Research" (paper presentation, 10th Australasian Conference on Information Systems, Wellington, New Zealand, December 1–3, 1999).
27. R. Luppicini, "Illuminating the Dark Side of The Internet with Actor-Network Theory: An Integrative Review of Current Cybercrime Research," *Global Media Journal* 7 (June 2014): 35–49.
28. R. D. Stachel and M. DeLaHaye, "Security Breaches in Healthcare Data: An Application of the Actor-Network Theory," *Issues in Information Systems* 16, no. 2 (2015): 185–194, https://doi.org/10.48009/2_iis_2015_185-194
29. W. Pieters, "Representing Humans in System Security Models: An Actor-Network Approach," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* 2, no. 1 (2011): 75–92.
30. T. Balzacq and M. D. Cavelty, "Theory of Actor-Network for Cyber-Security," *European Journal of International Security* 1, no. 2 (May 2016): 176–198, https://doi.org/10.1017/eis.2016.8
31. A. Mol, "Ontological Politics. A Word and Some Questions," *The Sociological Review* 47, no. 1 (May 1999): 74–89, https://doi.org/10.1111/j.1467-954x.1999.tb03483.x
32. T. Liebetrau and K. K. Christensen, "The Ontological Politics of Cyber Security: Emerging Agencies, Actors, Sites, and Spaces," *European Journal of International Security* 6, no. 1 (February 2021): 25–43, https://doi.org/10.1017/eis.2020.10
33. S. E. Zeltmann, N. Gupta, N. G. Tsoutsos, M. Maniatakos, J. Rajendran, and R. Karri, "Manufacturing and Security Challenges in 3D Printing," *JOM* 68, no. 7 (May 2016): 1872–1881, https://doi.org/10.1007/s11837-016-1937-7
34. B. Ranabhat, J. Clements, J. Gatlin, K.-T. Hsiao, and M. Yampolskiy, "Optimal Sabotage Attack on Composite Material Parts," *International Journal of Critical Infrastructure Protection* 26 (September 2019): 100301, https://doi.org/10.1016/j.ijcip.2019.05.004
35. L. J. Wells, J. A. Camelio, C. B. Williams, and J. White, "Cyber-Physical Security Challenges in Manufacturing Systems," *Manufacturing Letters* 2, no. 2 (April 2014): 74–77, https://doi.org/10.1016/j.mfglet.2014.01.005
36. L. D. Sturm, C. B. Williams, J. A. Camelio, J. White, and R. Parker, "Cyber-Physical Vulnerabilities in Additive Manufacturing Systems: A Case Study Attack on the .STL File with Human Subjects," *Journal of Manufacturing Systems* 44, Part 1 (July 2017): 154–164, https://doi.org/10.1016/j.jmsy.2017.05.007
37. A. E. Elhabashy, L. J. Wells, and J. A. Camelio, "Cyber-Physical Security Research Efforts in Manufacturing – A Literature Review," in *The 47th SME North American Manufacturing Research Conference* (Amsterdam, the Netherlands: Elsevier, 2019), 921–931, https://doi.org/10.1016/j.promfg.2019.06.115
38. D. Morris, G. Madzudzo, and A. Garcia-Perez, "Cybersecurity Threats in the Auto Industry: Tensions in the Knowledge Environment," *Technological Forecasting and Social Change* 157 (August 2020): 120102, https://doi.org/10.1016/j.techfore.2020.120102
39. S. Jothee, M. S. Shafie, and F. M. Nor, "Fatal Penetrating Neck Injury Due to Defective Airbag Inflator," *Forensic Science International* 291 (October 2018): e4–e7, https://doi.org/10.1016/j.forsciint.2018.08.038
40. "Takata Recall Spotlight," NHTSA, 2017, http://web.archive.org/web/20211009185128/https://www.nhtsa.gov/equipment/takata-recall-spotlight