Prevention and Mitigation of Disruptions in Medical Device Supply Chains: A Policy Perspective

Aman Goswami[1], Alok Baveja[2], Benjamin Melamed[2], Fred Roberts[3]

[1]Rutgers University, Department of Supply Chain Management, Newark, New Jersey, USA
[2]Rutgers University, Department of Supply Chain Management, Piscataway, New Jersey, USA
[3]Rutgers University, DIMACS, CCICADA, Piscataway, New Jersey, USA
https://doi.org/10.38126/JSPG240108
Corresponding author: ag1814@business.rutgers.edu
Keywords: medical device supply chain; medical device safety and security; cybersecurity; disruptions in medical devices; disruption classification; disruption prevention and mitigation

Executive Summary: New technologies and their connectivity to the internet render medical devices and their supply chains a target for worldwide criminal attacks. Disruptions to a *medical device supply chain* (MDSC), including cybersecurity attacks, have increased rapidly, with some sophisticated attacks compromising the availability and operation of life-critical devices. Understanding the impact of disruptions on MDSCs is difficult due to the attendant supply chain complexity. The lack of a systematic classification of disruptions to MDSCs limits the transferability of mitigation strategies. Thus, there is a need for evidence-based, actionable policy guidance for corporations and government agencies that address disruption risks to MDSCs. This paper first presents a disruption classification scheme based on historical and anticipated disruptions to MDSCs. Then, we introduce a model, dubbed the *Focal-firm Supply-chain Integrated Model* (FSIM), that integrates a focal-firm view of supply chains and attendant disruptions, illustrated through an MDSC example. Based on lessons learned from constructing a disruption classification and creating an FSIM map, we describe the following actionable insights: a) implementing procedures and technologies that enable early-detection of disruptions, b) accurate and timely information flows, c) continual monitoring of physical inventory levels and comparing them with digital data, d) enhanced and repeated testing at various supply chain testing sites, e) standardized metrics that measure the impact of disruptions, f) developing in advance a preparedness strategy and a planning process to allocate resources effectively, equitably, and transparently during disruptions, and g) the need for a common framework that bridges the medical device regulatory gaps across countries. These insights can guide MDSC stakeholders, including manufacturers, suppliers, service providers, healthcare providers, policymakers, and government agencies.

I. Introduction

The COVID-19 pandemic was accompanied by increased disruptions impacting supply chains (Goel et al. 2021; Ozdemir et al. 2022; Xu et al. 2020; Chowdhury et al. 2021). The disruptions were due to supply shortages (Bookwalter 2021), quality issues (Fonseca and Azevedo 2020), criminal activities such as counterfeiting (Shen et al. 2021), and cyberattacks (Pranggono and Arabo 2021), among others. Medical device supply chains (MDSCs) are a case in point. In this paper, we classify MDSC disruptions, describe a model built to understand them, and provide a variety of insights and conclusions about mitigating the impact of such

disruptions. This section discusses criminal disruptions to supply chains, the regulatory landscape of medical devices, and the need for a holistic approach to MDSC disruptions.

i. Criminal Disruptions To Supply Chains

Even before the COVID-19 pandemic, there was a growing trend of organized criminal activities falsifying medical devices, including a billion-dollar Medicare fraud scheme in the US (United States of America) involving medical professionals and telemedicine companies using telemarketing operations to target senior citizens with fraudulent and illegal orthotic braces (HHS 2019). At the start of the COVID-19 pandemic, there was a notable worldwide increase in the trafficking of falsified medical products (World Health Organization 2020). Furthermore, criminal agents increased their theft and counterfeiting efforts to disrupt MDSCs (Hodgkinson and Andresen 2020; Boman and Gallupe 2020). Examples include adulterated and misbranded COVID-19 tests and collection kits (Sridharan and Sivaramakrishnan 2023), fake personal protective equipment (PPE) kits (Lallie et al. 2021), and fake masks (Livingston et al. 2020). In addition, there have been several cyberattacks, such as ransomware, malware, and data breaches of hospital systems and medical device companies (Muthuppalaniappan and Stevenson 2021; Pranggono and Arabo 2021).

Some brazen attacks have caused considerable harm to the healthcare ecosystem's safety and security, and adversely impacted the availability of medical devices. A reliable medical device should be able to perform a requisite function under stated conditions without failure and operate for a specific time (Fries 2012). The growing shortage of semiconductor chips (Leslie 2022), a key component of medical devices, has exacerbated the problem of the supply of reliable medical devices. To address this shortage strategically, the US legislated the CHIPS and Science Act (The White House 2022) to incentivize domestic manufacturing, strengthen American supply chains, and enhance national security.

MDSCs are especially vulnerable to disruptions for the following reasons: (a) the complexity of the web of original medical device equipment manufacturers, healthcare delivery organizations, independent service organizations, and the network of regulatory and compliance agencies, (b) the use of legacy technology and outdated systems, (c) the integration of medical devices with clinical systems, which creates multiple points of vulnerability, (d) the vulnerability of modern software systems to cyber-attacks, and (e) challenges presented by data collection and maintenance. Medical devices have become increasingly connected to hospital systems and internet networks. They can also be implanted, sometimes with the ability of being remotely controlled by patients or their physicians. With the increased reliance on digital technologies, the points of vulnerability in medical devices and their supply chains have become alarmingly high (Sametinger et al. 2015). Therefore, there is a need for a deep understanding of MDSCs, including their internal processes, external linkages, testing and compliance, end-users, as well as their disruptions and mitigation strategies (Miller et al. 2021; Marucheck et al. 2011).

ii. Regulatory Landscape Of Medical Devices

Given the increasing sophistication and importance of medical devices, various medical device regulators joined forces in 2011 to create the International Medical Device Regulators Forum (IMDRF). The IMDRF comprises international members such as the US (Food and Drug Administration), South Korea (Ministry of Food and Drug Safety), and Europe (European Commission Directorate-General for Internal Market, Industry, Entrepreneurship, and Small and Medium Enterprises). The group releases internationally agreed-upon recommendation documents, which are then modified and adapted to meet the regulatory requirements of individual countries. Thus, the policies within the IMDRF are broad, and additional guidance is required for their implementation. In 2014, the World Health Organization (WHO) adopted a resolution strengthening the regulatory system for medical products designed to achieve better health outcomes (World Health Organization 2017), and the WHO acts as an official observer of the IMDRF. While the regulatory requirements, including the classification of medical devices, differ across countries, the coalition of regulators has come together to ensure a joint worldwide focus on health outcomes.

The regulation of medical devices involves competing goals of safety versus speedy approval processes. Europe and the US regulate medical

devices differently. The European Medical Device Regulation (MDR) is a set of regulations that govern the production and distribution of medical devices in Europe, requiring compliance by all medical device manufacturers intending to sell medical devices in Europe. In the US, the Food and Drug Administration (FDA) is the sole government authority regulating all medical devices in the US under the Federal Food, Drug, and Cosmetic (FD&C) Act. In contrast, the EU (European Union) follows a "Notified Body" system, where 38 member-state bodies (as of 2023) are designated under the MDR. In the past, both the EU MDR and the US FDA have been criticized for their different regulatory policies. The EU MDR has been criticized for its speedy decentralized device approval, which may unintentionally lead to more "fake" devices in the market. On the other hand, the US FDA has been criticized for its slow approval, compliance, and regulation of medical devices.

A decentralized system (such as the one followed in the EU) has the advantages of greater efficiency, a shorter device approval process, and a faster time to market, while a centralized system (such as the one followed in the US) has the advantages of standardized compliance procedures, better safety measures, and ease of acquisition of safety data. This dichotomy is evident in how these two bodies have regulated medical devices. The US FDA's primary purpose of regulating medical devices is borne out of its role as a public health agency aiming to curb the problem of fake and harmful devices. In contrast, the EU MDR's primary purpose is to foster innovation with effective commercial and industrial policies across nations (Van Norman 2016).

Medical devices are typically subject to controls specified by individual nations. These controls encompass the safety and efficacy of medical devices and ensure that the devices are not adulterated or misbranded. This makes the regulation of medical devices across the world heterogeneous and lacking in consistency. The WHO has taken strides to suggest a more consistent and streamlined approach to regulation by publishing international regulatory guides. Further, the Global Harmonization Task Force, a voluntary group comprising members from national regulatory authorities and industry from the EU, US, Japan, Australia, and Canada, was founded in 1992 to address the growing need for consistency in medical device regulation.

While the regulatory controls are commensurate with the level of risk associated with a medical device, there can be some differences in the pre-market requirements for medical devices across regulatory bodies of different countries. For example, all medical devices in the US are subject to general controls specified in the FD&C Act (FDA 1976) and classified by the FDA as per the risk the device poses to the patient as follows: Class I (low risk; e.g., bandages, handheld surgical instruments, stethoscopes, etc.), Class II (intermediate risk; e.g., computed tomography scanners, intravenous pumps, ventilators, etc.), and Class III (high risk; e.g., pacemakers, brain stimulators, implanted prosthetics, etc.). The devices also vary in the complexity of the technology used. In increasing order of technological sophistication, the types are *Disposables* (e.g., bandages, rubber gloves, etc.), *Surgical Instruments* (e.g., forceps, scissors, etc.), *Therapeutics* (e.g., cardiac pacemakers, infusion pumps, etc.), and *Diagnostic Equipment* (e.g., MRI machines, X-ray machines, etc.) Such a risk-based classification approach is also followed in the European Union, but with more classes (four categories of devices) and stricter delineation of the responsibilities of the economic operators and notified bodies, along with a difference in how connected devices are classified (Court 2021).

Further, individual countries develop their own regulatory documents and collaborate with various regulatory bodies to enhance the security of medical devices. For example, in 2003, the US FDA published the Quality System Regulations document to address device design, validation, and good manufacturing practices. Subsequently, amendments were made to add to the cybersecurity guidelines. Other US compliance and regulatory bodies, such as the Cybersecurity and Infrastructure Security Agency and the National Institute of Standards and Technology, also collaborate with the FDA to enforce guidelines that protect patients from medical device misuse. One of the key goals of the FDA's 'Resilient Supply Chain Program for Medical Devices' is to "identify supply chain risks and provide actionable information on those risks to medical device manufacturers, medical device distributors, healthcare delivery organizations, patients, healthcare workers, and government partners" (FDA 2022b).

iii. The Need For A Holistic Approach To MDSC Disruptions

Supply Chain Risk Management is a growing discipline. While substantial work has been done in risk classification (Rangel et al. 2015; Hudnurkar et al. 2017), there is limited research in the healthcare sector from a supply-chain risk-management perspective (Senna et al. 2020). Most research in healthcare supply chains aims to combat counterfeit medical devices (Clauson et al. 2018). However, focusing only on counterfeiting is not sufficient. A broader and more holistic understanding of disruptions that considers the diversity, impact, and mitigation strategies for all disruptions of medical devices is needed.

While there is relevant work (Thimbleby 2013; Mattox 2012; Polisena et al. 2014; Feldman et al. 2008; FDA 2023a), a supply chain perspective that incorporates disruptions to guide policies is missing. From a policy perspective, understanding large and complex healthcare systems has become increasingly difficult (Uzsoy 2005). Therefore, it is critical to map the end-to-end supply chain under study since visibility is a key determinant in managing supply chain risks (Ivanov 2021). Developing supply chain maps at the right level of granularity can lead to invaluable insights into risks and vulnerabilities. Furthermore, it is important to focus on a specific stakeholder's perspective. Existing granular supply chain maps, such as value stream maps or process maps, may not capture the extended supply chains (primarily upstream of a focal firm), where disruptive vulnerabilities often originate (MacCarthy et al. 2022). Therefore, it is not only important to derive actionable insights by taking a specific firm-centric view but also to incorporate the points of vulnerability associated with the extended supply chain.

To this end, this paper first develops a classification scheme that provides a taxonomy of MDSC disruptions and their impacts, and then presents corresponding mitigation strategies. We introduce a methodology that creates a model that integrates a focal-firm view of supply chains with disruptions. Dubbed *Focal-firm Supply-chain Integrated Model* (FSIM), this model includes a supply-chain map of a focal firm of interest and its external linkages as well as attendant disruptions. The FSIM methodology models the focal company in some detail and aggregates entities surrounding it to keep modeling complexity at a manageable level. Importantly, the various categories and locations of potential disruptions are directly integrated into the FSIM map. The classification of the disruptions and the development of the model were carried out in collaboration with industry experts (supply chain and security). These experts verified the created FSIM as well as its disruption classification. Finally, we present some insights, gleaned from the model, and make policy recommendations to MDSC stakeholders, including manufacturers, suppliers, service providers, healthcare providers, policymakers, and government agencies.

II. Unique Challenges of The Medical Device Industry

The global medical device industry is valued at USD 489 billion (Fortune Business Insights 2022a), with over 36% of this market in the US in 2021 (Fortune Business Insights 2022b). Medical devices include a broad category of technologies, such as thermometers, surgical supplies, gloves, syringes, PPE kits, pulse oximeters, implanted medical devices, cardiac pacemakers, ventilators, and in-vitro diagnostic devices (FDA 2022a). Medical devices are "…intended to affect the structure or any function of the body of man or other animals…" (FDA 2023b). Overall, the medical device industry is highly regulated, and compliance is of the utmost importance to manufacturers, since human and animal health and safety are at stake (Kramer et al. 2020; Jarow and Baxley 2015).

A key component of medical devices is the semiconductor chip (Semiconductor Industry Association 2021). Almost 50% of all medical devices have a semiconductor chip (Bradley 2022). These chips control operations, data processing, input and output management, sensing, wireless connectivity, and power management. An aging population, the rise of telehealth, the move to more portable and wearable devices, and the rise of artificial intelligence all contribute to the growth of the medical device semiconductor segment (Semiconductor Industry Association 2020).

Service and repair are other critical aspects of the medical device industry. Medical device manufacturers, third-party service organizations, and non-original equipment manufacturers can

service medical devices. To address security risks, healthcare delivery organizations get regulatory bodies' authorization to implement software and patch updates to medical devices. Such software updates are especially critical in addressing cybersecurity vulnerabilities (Digital Health Center of Excellence 2022). More generally, under Title 21 Code of Federal Regulations (CFR) Part 807, the FDA states that medical devices must meet FDA's regulations, regardless of whether the device is foreign made or domestically made (ECFR 2024).

Akin to the pharmaceutical industry, a distinctive characteristic of the medical device industry is the high inventory levels of products and components held by manufacturers. It is typical for medical device manufacturers to carry 150-400 days of inventory (Johnson 2022).

III. A Classification of Disruptions to MDSCs

Supply chain disruptions are defined as "unplanned and unanticipated events that disrupt the normal flow of goods and materials within a supply chain" (Craighead et al. 2007). The medical device industry has experienced a variety of security-related incidents and disruptions (Burns et al. 2016). For example, WannaCry ransomware and Ryuk ransomware targeted healthcare delivery organizations, causing widespread disruptions (Walker-Roberts et al. 2018). Furthermore, when Barnaby Jack, a cyber-security expert, demonstrated at the McAfee FOCUS 11 conference in 2010 how to hack an insulin pump that remotely altered the insulin dosage for a patient, an immediate global alert was issued concerning the vulnerabilities of medical devices (Beavers et al. 2019).

The disruption classification scheme presented in this section was developed through a literature review of historical medical device disruptions and in consultation with industry experts, supply chain researchers, and government agencies, such as the US Department of Homeland Security (DHS). The validity of each category was confirmed by the experts, and categories that could depict potential disruptions were incorporated into the classification scheme. Specifically, fourteen standardized categories based on a review of 70 historical incidents and potential incidents are depicted in Table 1. For further description and discussion of each disruption category, see the Appendix.

The industry and security experts who were involved in assisting and validating this classification all agreed that the medical device industry would be confronted with an escalation of disruptive attacks by criminal individuals or organizations. Disruptions are often viewed in a reactive, ad-hoc manner, thereby limiting lessons that could be learned from past incidents. Thus, it is important to compile a comprehensive classification of MDSC disruptions, which is lacking in the literature. The categorization presented in this section should help researchers and industry professionals to better understand threats and develop mitigation strategies related to medical devices.

Table 1. Classification of Disruptions to MDSCs (see Appendix for further details)

Disruption Category	Description	Example
1. Manufacturing Flaws or Adulteration	This category encompasses medical devices characterized by design flaws, faulty components, or contamination	Sale of adulterated and unapproved Supartz Euflexxa, Synvisc, Synvisc-One, and Orthovisc, which are hyaluronic-acid medical devices (DOJ 2021a)
2. Semiconductor Chip and Rare Earth Metal Shortage	This category describes the scarcity of semiconductor chips and rare earth metals used in several medical devices	Revenue loss at Philips (Flaherty 2022), and Hologic (Pederson 2022) due to chip shortages
3. Counterfeit Devices	This category encompasses any counterfeit of a container, packaging, labeling of a medical device or its components, as well as using a design masquerading as a genuine medical device	More than 250,000 counterfeit SURGICEL units (an Ethicon product) were sold to a wholesaler in Florida, USA (Albiani 2021)

4. Internal Theft	This category pertains to theft within facilities owned by the focal firm	Kevin Rumph, Jr. used a US Department of VA credit card to buy over $1.9 million worth of airway pressure equipment (DOJ 2021b)
5. External Theft	This category pertains to theft external to facilities owned by the focal firm via trash-diving to get discarded packaging or product material	The "Endoscopy Gang" of Spain sold stolen endoscopy probes on the Colombian black market (Carranco and Castedo 2013)
6. Transportation Theft	This category pertains to thefts while products or parts are being transported across facilities	Transport of stolen goods over $2.2 million from Johnson & Johnson subsidiaries in the infamous "Operation Miami Device" (Crotti 2016)
7. Unavailable or Improper Servicing	This category refers to potential disruptions stemming from improper servicing due to inadequate training or unavailability of servicing	Examples not recorded
8. Provider Kickbacks	This category pertains to kickbacks to healthcare providers for overuse of medical devices	Shire Pharmaceuticals used kickbacks to induce healthcare providers to overuse Dermagraft (DOJ 2017)
9. Distributor Kickbacks	This category pertains to kickbacks paid by a focal company to its distributors to switch to its products from those of competitors	Bayer Healthcare paid its distributors kickbacks to switch to Bayer products from those of competitors (DOJ 2008)
10. Billing for Unnecessary Medical Equipment	This category encompasses fraudulent or fake medical companies that harvest patient information and bill Medicare for fraudulent healthcare	Patsy Truglia bribed doctors in Florida to prescribe unnecessary medical braces to Medicare patients (DOJ 2022)
11. Packaging, Labeling, Misbranding, Unapproved, and Off-Label Use of Medical Devices	This category pertains to packaging defects, labeling errors, misbranding of content, incorrect features, and off-label use of a medical device for purposes other than intended	Olympus recalled 26,000 disposable EndoTherapy devices because a packaging defect affected their sterility (Crotti 2021)
12. Cyberattacks	This category encompasses attempts to steal, disrupt, alter, disable, or destroy information through ransomwares, device encryption, and remote hacking of implantable medical devices (IMDs)	The "WannaCry" ransomware attack infected the Bayer Medrad medical device, which is used to assist in MRI scans (Brewster 2017)
13. Natural Disasters and Power Outages	This category pertains to natural and climatic events that disrupt the functioning of medical devices	David Taylor, a ventilator patient, had to be transported to a hospital since the backup battery ran out of charge following a power outage (Huff 2021)
14. Supply Shortages	This category refers to supply shortages of medical devices that occur due to spikes in demand or loss of supplies	Shortage of blood bank supplies, which are in-vitro medical devices (Gavin 2022)

IV. The Focal-firm Supply-chain Integrated Model (FSIM)

In this section, we introduce a methodology that creates a model, dubbed *Focal-firm Supply-chain Integrated Model* (*FSIM*), which integrates a focal-firm view of a supply chain and attendant disruptions. A focal firm of an FSIM is a medical devices company of focal interest. More specifically, in FSIM there are two types of components: the focal company, which is modeled in detail, and all other components external to it (e.g., suppliers and customers), which are aggregated in the model to achieve a balance between modeling accuracy and manageable complexity. The choice of the focal-firm view comports with the modeling and analysis approach of the Theory of Constraints, which always starts the analysis of a system by articulating a clear goal of performance improvement (Goldratt and Cox 1984). This section further discusses gleaned actionable insights into MDSCs, conducive to making policy recommendations, obtained from constructing an FSIM map.

i. The FSIM Methodology

The FSIM methodology was employed by our research team of supply chain modelers in collaboration with industry and security experts. It consisted of three phases: (1) assembly of an advisory group of experts, (2) construction of a model of the medical device supply chain of interest, including an FSIM map, and (3) compiling a list of pertinent disruptions and integrating them on the FSIM map. Specifically, in phase 1, we assembled an advisory group of experts in supply chain management and security, including senior supply chain executives at a US medical devices firm. In phase 2, the research team conducted interviews with the advisory group to construct the supply chain model structure and obtain model parameters. The modeling task was performed as an iterative process, where at each iteration, the latest supply chain map was shown to the advisory group to seek feedback and suggestions for improvement. At every iteration, the validity and completeness of the information obtained was confirmed by all members of the advisory group. Finally, in phase 3, we proceeded to compile a list of pertinent disruptions. To this end, a literature review was conducted to understand past medical device disruptions. These disruptions were classified into categories and overlayed on the FSIM map. The advisory group reviewed the disruptions and confirmed their validity. The final iteration of the FSIM map is shown in Figure 1.

This model and FSIM map were developed for a large medical device company, to be referred to as MedTech Company, which serves as the focal firm. The individual elements of the FSIM map are described next (see CCICADA 2023 for more details):

1. The MedTech Company manufactures two types of products: Electronic Equipment (EE) and Delivery Systems (DS). EE units comprise medical devices with electronic components, software, semiconductors, etc. DS units are single-use devices that convey a medical product into a patient (e.g., catheters).

2. Any facility (node) label that contains the word 'Pool' represents an aggregation (e.g., of suppliers, production processes, etc.). For example, the *Hospital/ Equipment Pool* in Figure 1 represents all hospitals serviced by this focal firm. Aggregating entities external to the focal company into pools simplifies the model map while still capturing the functionality and vulnerabilities of the supply chain.

3. Gray icons represent internal processes at focal-firm facilities. For example, the *DS Production & Sterilization* node models the production process of DS units.

4. Green icons represent trusted focal-firm suppliers, while red icons represent untrusted focal-firm suppliers.

5. Blue arrows represent physical-flow transport routes of goods among facilities, while red arrows represent transport routes of untrusted flows (possibly including counterfeit items). Black arrows represent zero-delay information flows (e.g., supply orders).

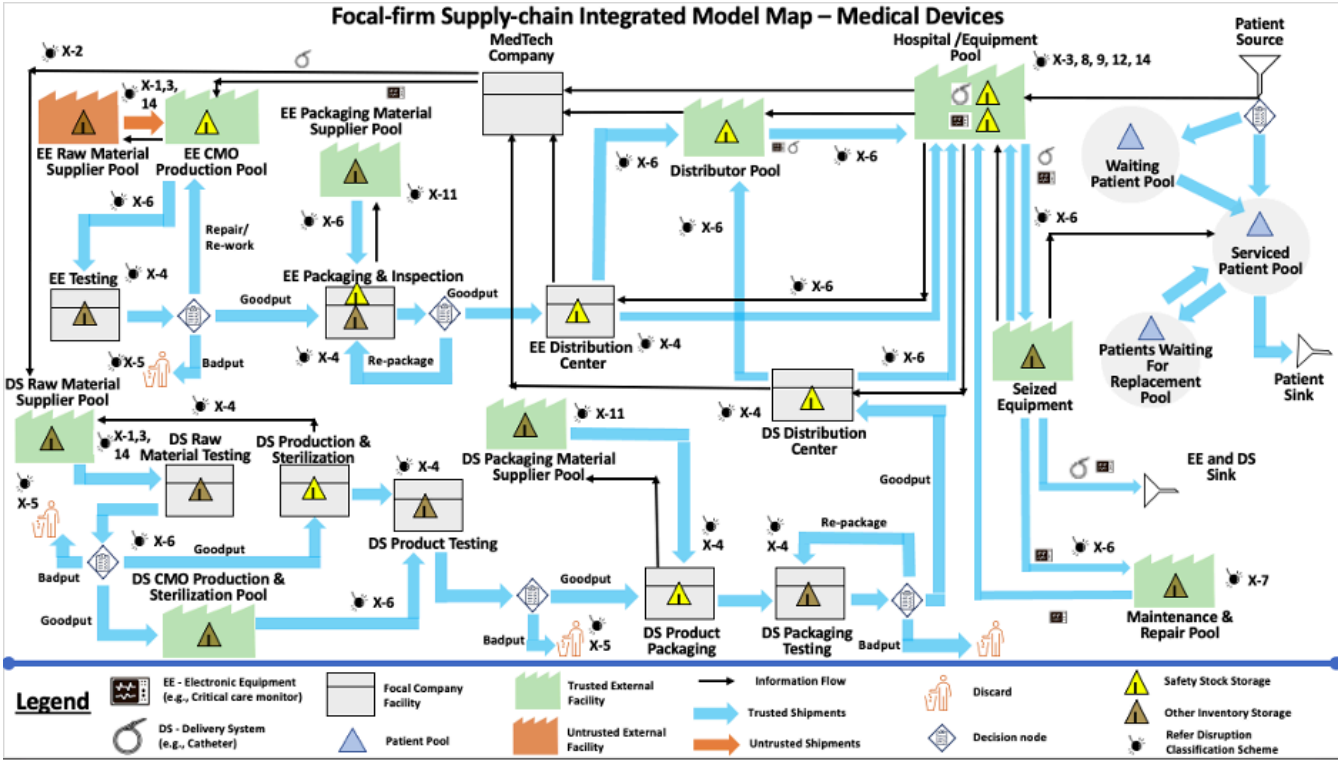
6. Yellow triangle icons represent safety stocks (e.g., at the *EE Packaging & Inspection* node), and beige triangle icons represent

other inventory storage (e.g., at the *DS Product Testing* node).

7. Blue triangle icons represent pools of patients at a hospital.

8. Finally, disruptions at various map locations (nodes and arrows) are represented each by an 'exploding-bomb' icon with disruption-code labels of the form 'X-1' to 'X-14', where X-n designates a disruption of class n according to the classification described in Section III.

Figure 1. FSIM Map of a MedTech Company



The FSIM methodology has two key merits. First, it facilitates understanding of supply chain operations, and by overlaying disruptions on the FSIM map, disruptions and impacts are clarified, thereby facilitating devising mitigation strategies. In particular, for each possible disruption, the FSIM map visualizes the disruption's onset location and its impact on the downstream supply chain. It further facilitates estimating the time to detect the disruption and mitigating it. For example, if we consider the disruption due to packaging defects that compromise the sterility of medical devices, such a disruption would likely occur at the *EE Packaging Material Supplier Pool* node or the *DS Packaging Material Supplier Pool* node. The disruption would be detected during inspection and testing at the *EE Packaging & Inspection* node, or the *DS Packaging Testing* node. Mitigation strategies would involve repackaging, or destruction to prevent misuse, as well as investigating the root cause for remedies.

The FSIM methodology can serve as a roadmap for MDSC companies with strong research expertise and modeling capabilities to create their own maps to understand the impact of disruptions and develop mitigation strategies. Furthermore, its generality makes it applicable to a wide range of industries, beyond medical devices. Indeed, we have successfully used this methodology to analyze supply chain models from diverse industries, such as pharmaceuticals, solar arrays, and food processing.

ii. Insights and Limitations

The process of constructing an FSIM map, including discussions with industry experts, led to several important insights. First, MDSCs rely on safety-stocks inventories for supply chain

resilience, and the associated replenishment policies (e.g., order size, reorder point, safety stocks, and lead time), which are critical management tools. Second, prevention or mitigation of disruptions depend on reliable system-wide data that can be leveraged to detect anomalies. Reliance solely on finished-goods inventory data could temporarily mask disruptions in progress, and result in delayed detection. Third, contract manufacturing organizations (CMOs) augment MDSCs' capacities, and require vigilance concerning their trustworthiness and security procedures. Fourth, while extensive testing is conducted on work-in-progress (WIP), such as materials, and packaging at various nodes of the MDSC, there is a continual need to monitor the reliability and efficacy of the testing process itself. Finally, data reliability is critical in ensuring the smooth and compliant functioning of the MDSC. Any cyberattack disruption to data integrity and reliability could have serious consequences, given the regulated nature of the industry.

Like any model, FSIM has its limitations. First, the process of developing such a model with adequate accuracy relies on collaboration with supply chain and security experts, typically drawn from industry. However, the availability and knowledge of such experts is often limited due to the distributed nature of the requisite knowledge. Second, knowledge on facilities, located in upstream tiers of the focal firm, is often scarce, and its paucity necessitates a judicious aggregation of such facilities into pools. Consequently, the identity of individual pool components is lost, and they cannot be analyzed individually. Third, in the absence of reliable data, the modeler often makes assumptions, which may not be adequately representative of reality. Finally, FSIM, represented as a simulation model with random components having probabilistic distributions, gives rise to experimental error in its statistical outputs, which must be controlled by time-consuming multiple simulation runs (replications).

V. Policy Recommendations

The FSIM methodology presented in this paper is specifically designed to help glean actionable insights by taking the viewpoint of a focal firm and incorporating the various disruption categories into the FSIM map. These insights facilitate the development and formulation of several important policy recommendations.

i. Early Detection of Disruptions

A key strategy for mitigating disruptions is maintaining high safety-stocks levels and end-product inventories (Tang 2006). However, high inventory levels and a primary focus on end-product inventories often mask early detection of disruptions; early detection and rapid response are important ways to limit the scale and scope of disruptions (Sheffi 2015). High inventory levels and only paying attention to end-product inventory can give rise to complacency that impedes the recognition of early warnings and rapid-response mindset (Tomlin and Wang 2011). Accordingly, we make the following recommendations for early detection of disruptions in MDSCs:

1. As part of preparedness activities, analyze the supply chain for points of vulnerability. The FSIM methodology could be used to this end.

2. Devise policies that disclose medical device disruptions, especially during public health emergencies.

3. Implement procedures that diversify suppliers and maintain adequate safety stocks.

4. Adopt technologies that enable early detection of disruptions through real-time warning systems across the supply chain that trigger a rapid response (e.g., investigation and mitigation). To this end, developing remote monitoring capabilities and enabling real-time tracking of medical device performance can further enhance early detection of disruptions.

ii. Effective Information Flow Management

This policy recommendation relates to information flows. Information flows in MDSCs support the physical flows. Further, these flows are critical in ensuring compliance with regulatory agencies. Accordingly, we make the following recommendations for effective information flows:

1. MDSCs should carefully manage and maintain information flows for accuracy and timeliness.

2. MDSCs should devise standard protocols of data exchange and integrate medical devices with health IT systems in order to improve informational flow management. It is important to ensure that the informational flow management processes comply with all applicable medical device regulations.

The FSIM methodology provides a deeper understanding of information flows within MDSCs. For example, to maintain timely availability of finished goods to end-customers, the EE/DS production processes described in Section IV need to be synchronized and coordinated to produce medical kits (one EE and one DS per incoming patient).

iii. Building Cyber-Resilient MDSCs

While much effort has focused on reducing risks associated with physical entities of the supply chain, less attention has been paid to developing cyber-resilient supply chains. A cyberattack on the information infrastructure of MDSCs can disastrously impact the physical flows and jeopardize regulatory compliance. Recovery from compromised compliance is difficult, time-consuming, and can have long-term consequences on sales due to reputational damage to the brand (UBS 2021; Medical Plastic News 2022). Given the importance of cybersecurity, we make the following recommendations for cyber-resilient MDSCs:

1. MDSC stakeholders should allocate and deploy adequate resources to monitor physical flows and inventory levels and compare them with digital data to detect data breaches as early as possible. These resources would include cybersecurity personnel with strategic and operational expertise. Right-sizing cybersecurity budgets is nuanced, being a function of the size and complexity of the organization as well as the type of products and services offered by the organization. As a rule of thumb, it is recommended that the cybersecurity budget should be between 7% and 20% of the total IT budget (SenseOn 2023).

2. MDSCs should set up advanced security operations centers (SOCs) that plan, monitor, and respond to security threats.

3. MDSCs should develop and disseminate cybersecurity policies along with detailed guidelines for threat identification and response playbooks leveraging MDSC consortia, such as Medical Device Manufacturers Association (MDMA) and Medical Device Innovation Consortium (MDIC).

4. MDSCs should establish ongoing cybersecurity training programs that match the employees' levels of responsibility. Training topics should include basic cyber hygiene for all employees, identifying early warnings of cyberattacks and, nascent threats, as well as implementing prompt reporting and response procedures.

5. MDSCs should seek regular information about cybersecurity practices of vendors and suppliers outside the focal company and seek contractual agreements with them regarding such practices.

iv. End-to-End Testing

Risk assessment and checking the efficacy of testing protocols at various supply chain components is critical to medical device manufacturers. Well-designed testing plans help assess vulnerabilities of medical devices and point to appropriate mitigation strategies. Accordingly, we make the following recommendations for end-to-end testing in MDSCs and their suppliers:

1. Each component of an MDSC should develop comprehensive testing plans of device hardware, software, performance, safety, and usability.

2. Each component of an MDSC should have contractual agreements with its suppliers that stipulate comprehensive risk assessment and testing protocols.

v. Standardization of Metrics

MDSC stakeholders and policymakers need standardized quality and disruption metrics to compare vulnerabilities, mitigation strategies, and the impact of changes to a supply chain. Such metrics can be used by in-vitro simulation experiments in assessing disruption impacts, identifying vulnerabilities, and developing efficacious mitigation strategies, as well as comparing the efficacy of alternate changes. In addition, combining the standardization of disruption classification and disruption metrics can help guide policy decisions more effectively and systematically. Several ISO standards are applicable to medical devices, such as ISO 14971 (risk management), 10993 (biocompatibility), 62304 (medical device software), and 13485 (quality management). Recently, the FDA recognized the ISO 13485 international medical device quality management standard as part of its Quality Management System Regulation (QMSR). The creation and use of such standards globally is of vital importance. However, international standards for assessing the impact of disruptions are lacking. Accordingly, we recommend that global regulatory bodies also play a role in the development of metrics that quantify the impact of disruptions.

vi. Disruption Preparedness Strategy

The COVID-19 pandemic has highlighted a plethora of supply chain challenges on a global scale. In addition to widespread supply shortages, these challenges have further included equitable distribution/allocation, regulatory compliance, and oversight to ensure patients' health and safety. A recent investigative report on the lessons learned from this emergency by a group of leading national experts highlights the need for a preparedness strategy to rapidly produce and distribute medical devices so as to maximize societal benefits (The Covid Crisis Group 2023). Such a strategy should have a preparedness planning process for allocating scarce resources effectively, equitably, and transparently. Our current work uncovered an industry-wide emphasis on MDSC 'efficiency' (costs) and less so on 'effectiveness' (responsiveness). Responsiveness in these supply chains depends mainly on the availability of adequate inventory levels, which were not sized for large-scale emergencies. Accordingly, we recommend the following disruption preparedness strategy:

1. MDSCs should adopt a two-pronged supply chain strategy for two regimes: 1) an efficient supply chain that is used in normal regimes where supply and demand follow forecasts, and 2) a responsive supply chain ready to be deployed on short notice in emergencies. Such a rapid-response supply chain should have the following capabilities: (a) an ability to tap into excess capacity, shorten lead times, and deploy new resources for manufacturing and compliance, (b) an ability to rapidly and adaptively respond to shortages and disruptions through already developed contingency plans, and (c) an ability to rapidly detect and remove fraudulent/counterfeit products.

2. Since such proactive planning strategies call for a governmental policy that goes beyond inventories, and incentivizes MDSCs' preparedness for emergencies, governments should collaboratively lead the implementation of this strategy.

3. Governments should incentivize the development of global, industry-wide collaborative platforms to rapidly share information in case of emergencies and threats.

vii. Medical Device Safety

Ensuring the safety of medical devices is a central concern of MDSCs and regulatory agencies. However, the safety standards are not uniform across countries. Adopting a shared regulatory framework can go a long way toward ensuring medical device safety by assessing gaps in medical device regulations, workforce, and equipment management software used by various countries. Accordingly, we recommend that the provisions of the Global Harmonized Task Force (GHTF), the EU, and the US can serve as benchmarks for countries that do not have a comprehensive medical device regulatory system. To this end, data in the Global Atlas of Medical Devices (GMAD) can be leveraged to provide global, regional, and country-level data on the availability of national policy on health and technology, and regulation of medical devices,

including the use of medical device nomenclature systems. This policy recommendation, once implemented, would ensure medical device safety by globally harmonizing pre-market requirements and post-market surveillance to ensure consistency in the way medical device data is acquired and assessed.

viii. Barriers to Recommendation Implementation

It is important to recognize the key barriers to implementing these recommendations. For example, implementing technologies that enable early detection of disruptions requires changing the mindset of MDSC stakeholders from an "inventory-first" viewpoint to a "disruption-first" viewpoint. Understanding the location and severity of disruptions is essential to deploying efficacious mitigation strategies. While large levels of safety stocks can mitigate disruptions, they do not constitute a comprehensive solution to the problem of disruptions. Worse still, excessive safety stock levels may mask disruptions in progress. Monitoring for potential disruptions requires investments in sophisticated technology and cybersecurity expertise. Investments in security, and particularly cybersecurity, are often lower than investments in R&D, better infrastructure, and hiring more experienced employees. Moreover, deploying legacy medical devices that possess limited connectivity with modern detection capabilities can be challenging. Prioritizing investments in cybersecurity requires that the value of disruption prevention be well-understood by management. Further, implementing regulatory changes at all levels is a complex undertaking. It requires collaboration across multiple agencies, government bodies, regulatory authorities, and MDSC stakeholders in developing security and safety policies for medical devices. Some of these barriers can be overcome by developing cost/benefit analysis tools for MDSC stakeholders to support the identification of effective policies.

VI. Conclusion

MDSCs are part of the national—critical infrastructure since the products they deliver are vital to public health and safety. Disruptions to the availability of MDSC products, such as PPE kits and ventilators, experienced during the COVID-19 pandemic, resulted in life-threatening societal consequences Thus, it is important to understand MDSC operations, the typology of attendant disruptions and their impacts, and to acquire the capability of devising mitigation strategies.

This paper presents the FSIM methodology for modeling the impact of disruptions to facilitate extracting actionable prevention and mitigation insights. It further demonstrates the importance of developing rigorous methodologies, tools, and processes to help craft better-informed policies. Specifically, this paper introduces a disruption classification for MDSCs that could assist in systematically creating a knowledge base to be used across locations, impacts, and mitigations. The disruption classification has been validated by industry experts and was used to overlay disruptions on an FSIM map.

The insights gleaned from this work indicate the need for MDSC stakeholders to implement policies, procedures, and technologies as follows: (i) enabling early-detection of disruptions by real-time and enterprise-wide warning systems, (ii) managing accurate and timely information flows, (iii) incorporating continual monitoring of physical and digital data into cyber-resilient supply chains, (iv) testing products extensively across the MDSC, (v) measuring disruptions via standardized metrics, (vi) adopting preparedness strategies that allocate resources effectively, equitably, and transparently during disruptions as well as developing industry-wide collaborative platforms that rapidly share information and adaptively respond to emergencies, and (vii) instituting a shared global framework to guide national regulatory policies for medical devices.

In summary, the medical device industry needs scientifically informed structuring that integrates policies, governmental regulations, metrics, and public-private collaboration across nations. The FSIM methodology, presented in this paper, can facilitate achieving this goal.

Appendix

Disruption category 1: '*Manufacturing Flaws or Adulteration*'. An example of a category 1 disruption is the supply of adulterated and unapproved, foreign-market products, such as Supartz Euflexxa, Synvisc, Synvisc-One, and Orthovisc, which are prescription hyaluronic-acid medical devices intended to treat knee osteoarthritis pain. Distributed by Affordable Healthcare Solutions, LLC, the value of these devices was over $800,000 (DOJ 2021a).

Disruption category 2: '*Semiconductor Chip and Rare Earth Metal Shortage*'. Two-thirds of all medical devices and over 50% of all connected devices use semiconductors (Bradley 2022). An example from this disruption category is the shortage of semiconductor chips leading to higher component prices for Philips, which sustained a hit of €120 million from their cost increase (Flaherty 2022). Another example is the company Hologic, which makes mammography and other imaging machines, and reported a $200 million revenue loss because of a chip shortage (Pederson 2022). In addition, rare earth elements (REE) are groups of metals with unique physical and chemical properties that are used in many medical device applications (e.g., gadolinium is used in MRI images, neodymium is used in hearing aids, zirconium is used for hemodialysis, etc.). These elements are difficult to mine due to environmental regulations and offer few substitutes. Western countries have typically relied on China for its abundance of rare earth elements. However, a shortage of such critical rare earth elements could significantly impact the medical device industry.

Disruption category 3: '*Counterfeit Devices*', which includes any counterfeit of a container, packaging, labeling of a medical device or its components, or using a design masquerading as a genuine medical device. For example, the COVID-19 pandemic witnessed an increase in fake testing kits, thermometers, pulse oximeters, masks, and other devices (Sridharan and Sivaramakrishnan 2023).'Operation Pangea', conducted by Interpol, found that over 50% of all medical devices seized in a certain week were fake testing kits, potentially worth more than $23 million. Another example involves a counterfeit SURGICEL product, made by Ethicon, a subsidiary of Johnson & Johnson, which is a hemostat used to control bleeding during surgical procedures. An illicit trader in Delhi, India and Dubai, UAE was responsible for supplying more than 250,000 units of counterfeit and contaminated SURGICEL and other Ethicon medical devices to a gray-market wholesaler in Florida. Intelligence from this operation aided another global law enforcement operation involving multiple countries to identify another gray-market wholesaler in Illinois and led to the seizure of over $25 million in other illicit medical devices (Albiani 2021). While counterfeit drugs are well-researched in the literature (Blackstone et al. 2014; Cockburn et al. 2005; World Health Organization 1999; Rudolf and Bernstein 2004; Eban 2006), there is limited knowledge and awareness of counterfeit medical devices (Mori et al. 2011).

Disruption categories 4, 5, 6: '*Internal Theft*' (e.g., stealing cargo from a facility owned by the focal firm), '*External Theft*' (e.g., trash-diving to get waste, discarded packaging, or product material), and '*Transportation Theft*' (e.g., cargo thefts during transportation across facilities), respectively. Stolen medical devices can also be introduced into legitimate supply chains via underground markets. Medical devices can also be altered, affecting their reliability. An example from the 'Internal Theft' category is the theft by Kevin Rumph, Jr, who used his US Department of Veteran Affairs credit card to buy over $1.9 million worth of airway pressure equipment, and then sold the unauthorized purchases to another vendor (DOJ 2021b). An example from the 'External Theft' category involves the "Endoscopy Gang" of Spain (Carranco and Castedo 2013), which stole endoscopy probes from various hospitals in Spain and sold them on the Colombian black market. An example from the 'Transportation Theft' category is the infamous 'Operation Miami Device' (Miami-based FDA investigation), where a former sales representative of Johnson & Johnson conspired with other sales representatives of Johnson & Johnson subsidiaries to transport stolen medical devices for a period of ten years and laundered over $2.2 million (Crotti 2016).

Disruption category 7: '*Unavailable or Improper Servicing*.' We could not find historical instances of

this disruption. However, we hypothesize that with the growing third-party servicing operations of medical device repair and maintenance, improper servicing caused by lack of proper training or unavailability of servicing (e.g., due to excessive demand) could result in a severe disruption (Vockley 2016). It is true that third-party entities may find it challenging to obtain device servicing manuals, technical specification documents, and quality replacement parts. Still, such third-party entities may also engage in a variety of unscrupulous activities, such as using substandard replacement parts, or manipulating the security controls of the medical device for privileged access during repair. In addition, information concerning the servicing history of medical devices is lacking, which makes it difficult for regulatory bodies to regulate them adequately (FDA 2018).

Disruption category 8, 9: '*Provider Kickbacks*' and '*Distributor Kickbacks,*' respectively. Medical device companies can use kickbacks or engage in cash-for-patient schemes, paying kickbacks to distributors for switching products for delivery to patients (Offices of The United States Attorneys 2012). Kickbacks alter medical device demand and supply, affecting end-users and other parts of the supply chain. An example of 'Provider Kickbacks' is the case of Shire Pharmaceuticals using kickbacks and other unlawful methods to induce healthcare providers to overuse one of its products called Dermagraft (DOJ 2017). An example of 'Distributor Kickbacks' is the case of Bayer Healthcare (manufacturer of diabetic self-testing supplies), which paid its suppliers kickbacks in return for suppliers switching patients from Bayer competitors' products to Bayer (DOJ 2008).

Disruption category 10: '*Billing for Unnecessary Medical Equipment*.' This category pertains to fake medical companies harvesting patient information and billing Medicare for fraudulent orders. An increase in such fake entities in the market impacts the supply of medical equipment, further affecting demand from legitimate entities. In addition to disrupting legitimate MDSCs, such disruptions divert funds that could be funneled to research or better care of patients. An example from this disruption category is the durable medical equipment scam and the subsequent 'Operation Brace Yourself' (HHS Office Of Inspector General 2022). One such incident occurred in Florida, where patients' personal and medical information was harvested from a telemarketing operation. Subsequently, doctors were bribed to subscribe unnecessary medical braces to Medicare recipients, and the perpetrator, Patsy Truglia, was able to amass $18.3 million from this scheme (DOJ 2022). In addition, unwanted overuse of medical services worldwide in countries like Australia, Iran, Spain, Brazil, etc., has become quite widespread in recent years (Brownlee et al. 2022). The overuse of screening tests, diagnostic tests, and end-of-life care gives rise to excessive demand for medical devices and equipment (real or fake), which may not be required at all. This demand leads to the proliferation of fake entities in the market to supply this equipment.

Disruption category 11: '*Packaging, Labeling, Misbranding, Unapproved, or Off-Label Use of a Medical Device*.' Companies sell products with packaging defects or labeling errors, distribute unapproved medical devices, or misbrand medical devices, leading physicians to use the off-label device in unapproved uses. A device can be misbranded by false or misleading labeling, missing labels, inaccurate statements about the content, weight, and features, inadequate directions of use, and non-compliance with the color-additive provisions as specified by regulatory bodies. An example from this category is the Olympus recall of 26,000 disposable EndoTherapy devices because of a packaging defect that affected the sterility of these devices. In addition, over 113 models were impacted because of a defective seal (Crotti 2021).

Disruption category 12: '*Cyberattacks*.' More than 1 in 3 healthcare provider facilities reported being hit by ransomware in 2020 (Pifer 2021). Cyberattacks have affected over 600 US healthcare organizations and more than 18 million patient records in 2020 alone at an estimated cost of nearly $21 billion (Weiner 2021). A recent Health-ISAC report, entitled 'Securing the Modern Pharmaceutical Supply Chain: A Guide for CISOs in an Age of Disruption', stressed *increasing concern about bad actors targeting operating technology (OT) systems used to run the manufacturing floor,*

labs, R&D facilities, warehouses, and distribution centers(Health-ISAC 2022). Cyberattacks on medical devices can be both passive (e.g., those that compromise a device's security and wrongfully obtain a patient's data) and/or active (e.g., those that directly threaten the well-being or life of a patient by targeting implantable medical devices such as pacemakers). Hackers can remotely take control of devices such as infusion pumps, insulin pumps, pacemakers, defibrillators, etc., and modify the functions of medical devices to cause harm to patient physiology. One of 27 examples of this disruption category in our database is the "WannaCry" ransomware attack. The ransomware impacted over 200,000 Windows systems, 48 hospital trusts in the UK, and various medical facilities in the US. Specifically, the Bayer Medrad medical device, which is used to assist in MRI scans was affected. Operations were restored in 24 hours. (Brewster 2017).

Disruption category 13: '*Natural Disasters and Power Outages*', which refers to climate scenarios disrupting the functioning of medical devices at homes or hospitals (Browning and Tuma 2015). An example of this disruption category is the power outages in Texas in February 2021. David Taylor, a patient who relied on a ventilator to breathe, had to be transported to a hospital after his ventilator's backup battery ran out of charge following a power outage. The growing medical device market requires more reliable power (Huff 2021).

Disruption category 14s '*Supply Shortages*. An example is shortage of blood bank supplies, which are classified as in-vitro medical devices. A critical shortage of blood supplies threatens the ability to provide transplants, surgeries, cancer therapies, etc. (Gavin 2022). The COVID-19 pandemic led to a dramatic excess of demand over supply for blood and its components due to canceled blood drives, fewer donors, and labor/staff shortages. From 2010 to 2019, there were five shortages of medical devices annually, with the first half of 2020 witnessing 20 shortages (Beleche et al. 2022).

References

Albiani, Roy. 2021. "Combating Counterfeit Medical Devices: A Case Study". Johnson & Johnson. https://bpp.msu.edu/magazine/combating-counterfeit-medical-devices-a-case-study-march2021/

Beavers, Jake L, Michael Faulks, and Jims Marchang. 2019. "Hacking NHS pacemakers: a feasibility study." 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3). https://doi.org/10.1109/ICGS3.2019.8688214

Beleche, Trinidad, Maria Kuecken, Aliya Sassi, Katherine Toran, Emily Galloway, and Thomas Henry. 2022. "Characteristics of Medical Device Shortages in the US, 2006–20: Study examines the characteristics of medical device shortages in the US from 2006–20." *Health Affairs* 41 (12): 1790-1794. http://doi.org/10.1377/hlthaff.2022.00643

Blackstone, Erwin A, Joseph P Fuhr Jr, and Steve Pociask. 2014. "The health and economic effects of counterfeit drugs." *American Health & Drug Benefits* 7 (4): 216. https://pubmed.ncbi.nlm.nih.gov/25126373/

Boman, John H, and Owen Gallupe. 2020. "Has COVID-19 changed crime? Crime rates in the United States during the pandemic." *American Journal of Criminal Justice* 45: 537-545. https://doi.org/10.1007/s12103-020-09551-3

Bookwalter, Christina M. 2021. "Drug shortages amid the COVID-19 pandemic." *US Pharm* 46 (2): 25-8. https://www.uspharmacist.com/article/drug-shortages-amid-the-covid19-pandemic

Bradley, Stephen. 2022. "How is the semiconductor shortage affecting medtech?". Deloitte Consulting LLP. https://www2.deloitte.com/us/en/blog/health-care-blog/2022/how-is-the-semiconductor-shortage-affecting-medtech.html.

Brewster, Thomas. 2017. "Medical Devices Hit By Ransomware For The First Time In US Hospitals." https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/

Browning, John G, and Shawn Tuma. 2015. "If your heart skips a beat, it may have been hacked: cybersecurity concerns with implanted medical devices." *SCL Rev.* 67: 637. https://scholarcommons.sc.edu/sclr/vol67/iss3/8

Brownlee S, Chalkidou K, Doust J, Elshaug AG, Glasziou P, Heath I, Nagpal S, Saini V, Srivastava D, Chalmers K, Korenstein D. 2022. "Evidence for overuse of medical services around the world." The Lancet, 390(10090), 156-168. https://doi.org/10.1016/S0140-6736(16)32585-5

Burns, AJ, M Eric Johnson, and Peter Honeyman. 2016. "A brief chronology of medical device security."

Communications of the ACM 59 (10): 66-72. https://doi.org/10.1145/2890488

Carranco, Rebeca, and Castedo Antia. 2013. "Endoscopy Gang caught by police with medical equipment worth 300,000". https://english.elpais.com/elpais/2013/09/06/inenglish/1378471243_834228.html

CCICADA. 2023. "Past, Active, or Planned Criminal Disruptions of Medical-Device Supply Chains." https://ccicada.org/2023/05/05/past-active-or-planned-criminal-disruptions-of-medical-device-supply-chains/

Chowdhury, Priyabrata, Sanjoy Kumar Paul, Shahriar Kaisar, and Md Abdul Moktadir. 2021. "COVID-19 pandemic related supply chain studies: A systematic review." *Transportation Research Part E: Logistics and Transportation Review* 148: 102271. https://doi.org/10.1016/j.tre.2021.102271

Clauson, Kevin A, Elizabeth A Breeden, Cameron Davidson, and Timothy K Mackey. 2018. "Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare: An exploration of challenges and opportunities in the health supply chain." *Blockchain in Healthcare Today*. https://doi.org/10.30953/bhty.v1.20

Cockburn, Robert, Paul N Newton, E Kyerematen Agyarko, Dora Akunyili, and Nicholas J White. 2005. "The global threat of counterfeit drugs: why industry and governments must communicate the dangers." *PLoS Medicine* 2 (4): e100. https://doi.org/10.1371/journal.pmed.0020100

Court, Laura. 2021. "How are medical devices classified under EU MDR?". https://www.greenlight.guru/blog/eu-medical-device-classification

Craighead, C.W., Blackhurst, J., Rungtusanatham, M.J. and Handfield, R.B. 2007. "The severity of supply chain disruptions: design characteristics and mitigation capabilities." *Decision Sciences, 38*(1), pp.131-156. https://doi.org/10.1111/j.1540-5915.2007.00151.x

Crotti, Nancy. 2016. "Former J&J Sales Rep Convicted in Stolen Devices Scheme." https://www.mddionline.com/former-jj-sales-rep-convicted-stolen-devices-scheme.

Crotti, Nancy. 2021. "Olympus recalls thousands of endo devices due to packaging defect." https://www.medicaldesignandoutsourcing.com/olympus-recalls-thousands-of-endo-devices-due-to-packaging-defect/.

Department of Justice (DOJ). 2008. "Bayer Healthcare to Pay U.S. $97.5 Million to Settle Allegations of Paying Kickbacks to Diabetic Suppliers." https://www.justice.gov/archive/opa/pr/2008/November/08-civ-1050.html.

DOJ. 2017. "Shire PLC Subsidiaries to Pay $350 Million to Settle False Claims Act Allegations." https://www.justice.gov/opa/pr/shire-plc-subsidiaries-pay-350-million-settle-false-claims-act-allegations.

DOJ. 2021a. "Medical Device Company Pleads Guilty to Dealing in Adulterated Devices, Forfeits Over $800,000 in Non-FDA Approved Devices." https://www.justice.gov/usao-sdfl/pr/medical-device-company-pleads-guilty-dealing-adulterated-devices-forfeits-over-800000

DOJ. 2021b. "Veterans Affairs employee pleads guilty to theft of medical equipment." https://www.justice.gov/usao-ndga/pr/veterans-affairs-employee-pleads-guilty-theft-medical-equipment.

DOJ. 2022. "South Florida Man Sentenced To 15 Years for Consecutive Health Care Fraud Conspiracies."https://www.justice.gov/usao-mdfl/pr/south-florida-man-sentenced-15-years-consecutive-health-care-fraud-conspiracies.

Digital Health Center of Excellence. 2022. "Cybersecurity Fact Sheet." FDA. https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity.

Eban, Katherine. 2006. *Dangerous doses: A true story of cops, counterfeiters, and the contamination of America's drug supply*. HMH.

eCFR. 2024. "Part 807 – Establishment registration and device listing for manufacturers and initial importer of devices." https://www.ecfr.gov/current/title-21/chapter-I/subchapter-H/part-807

Food and Drug Administration (FDA). 1976. "General Controls of Medical Devices." https://www.fda.gov/medical-devices/regulatory-controls/general-controls-medical-devices

FDA. 2018. "FDA Report on the Quality, Safety, and Effectiveness of Servicing of Medical Devices."

FDA. 2022a. "How To Determine if Your Product Is a Medical Device." https://www.fda.gov/medical-devices/classify-your-medical-device/how-determine-if-your-product-medical-device.

FDA. 2022b. "Resilient Supply Chain Program for Medical Devices." https://www.fda.gov/about-fda/cdrh-offices/resilient-supply-chain-program-medical-devices.

FDA. 2023a. "Medical Device Safety." https://www.fda.gov/medical-devices/medical-device-safety.

FDA. 2023b. "How FDA Regulates Animal Devices." https://www.fda.gov/animal-veterinary/animal-health-literacy/how-fda-regulates-animal-devices

Feldman, Mitchell D, Amy J Petersen, Leah S Karliner, and Jeffrey A Tice. 2008. "Who is responsible for evaluating the safety and effectiveness of medical devices? The role of independent technology assessment." *Journal of General Internal Medicine* 23: 57-63. https://doi.org/10.1007/s11606-007-0275-4

Fonseca, Luis Miguel, and Américo Lopes Azevedo. 2020. "COVID-19: outcomes for global supply chains." *Management & Marketing. Challenges for the Knowledge Society* 15 (s1): 424-438. https://recipp.ipp.pt/bitstream/10400.22/18641/1/ART_CIDEM_10.2478_mmcks_2020.pdf

Fortune Business Insights. 2022a. "Medical Device Market Size." Fortune Business Insights. https://www.fortunebusinessinsights.com/industry-reports/medical-devices-market-100085.

Fortune Business Insights. 2022b. "USA Medical Device Market Size." Fortune Business Insights. https://www.fortunebusinessinsights.com/u-s-medical-devices-market-107009.

Fries, Richard C. 2012. *Reliable design of medical devices*. CRC Press.

Gavin, Kara. 2022. "Bare shelves in the blood bank means threat to patient care." https://www.michiganmedicine.org/health-lab/bare-shelves-blood-bank-means-threat-patient-care.

Goel, Rajeev K, James W Saunoris, and Srishti S Goel. 2021. "Supply chain performance and economic growth: The impact of COVID-19 disruptions." *Journal of Policy Modeling* 43 (2): 298-316. https://doi.org/10.1016/j.jpolmod.2021.01.003

Goldratt, Eliyahu M, and Jeff Cox. 1984. *The Goal: Excellence in Manufacturing*. North River Press.

Health-ISAC. 2022. "Securing the Modern Pharmaceutical Supply Chain: A Guide for CISOs in an Age of Disruption." https://h-isac.org/securing-the-modern-pharmaceutical-supply-chain/.

Department of Health and Human Services (HHS). 2019. "Nationwide Brace Scam." https://oig.hhs.gov/fraud/consumer-alerts/fraud-alert-nationwide-brace-scam/.

HHS Office Of Inspector General. 2022. "Nationwide Brace Scam." https://oig.hhs.gov/newsroom/media-materials/nationwide-brace-scam/.

Hodgkinson, Tarah, and Martin A Andresen. 2020. "Show me a man or a woman alone and I'll show you a saint: Changes in the frequency of criminal incidents during the COVID-19 pandemic." *Journal of Criminal Justice* 69: 101706. https://doi.org/10.1016/j.jcrimjus.2020.101706

Hudnurkar, Manoj, Sujeet Deshpande, Urvashi Rathod, and Suresh K Jakhar. 2017. "Supply chain risk classification schemes: A literature review." *Operations and Supply Chain Management: An International Journal* 10 (4): 182-199. http://doi.org/10.31387/oscm0290190

Huff, Charlotte. 2021. "Growing Power Outages Pose Grave Threat to People Who Need Medical Equipment to Live." https://www.npr.org/sections/health-shots/2021/05/15/996872685/growing-power-outages-pose-grave-threat-to-people-who-need-medical-equipment-to-.

Ivanov, Dmitry. 2021. "Digital supply chain management and technology to enhance resilience by building and using end-to-end visibility during the COVID-19 pandemic." *IEEE Transactions on Engineering Management*. https://doi.org/10.1109/TEM.2021.3095193

Jarow, Jonathan P, and John H Baxley. 2015. "Medical devices: US medical device regulation." Urologic Oncology: Seminars and Original Investigations. https://doi.org/10.1016/j.urolonc.2014.10.004

Johnson, Stu. 2022. "7 Critical Best Practices for Medical Device Inventory Management." Rootstock Manufacturing ERP. https://www.rootstock.com/cloud-erp-blog/7-best-practices-medical-device-inventory-management/.

Kramer, Daniel B, Shuai Xu, and Aaron S Kesselheim. 2020. "Regulation of medical devices in the United States and European Union." In *The ethical challenges of emerging medical technologies*, 41-48. Routledge. https://doi.org/10.1056/NEJMhle1113918

Lallie, Harjinder Singh, Lynsay A Shepherd, Jason RC Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens. 2021. "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic." *Computers & Security* 105: 102248. https://doi.org/10.1016/j.cose.2021.102248

Leslie, Mitch. 2022. "Pandemic scrambles the semiconductor supply chain." *Engineering* 9: 10-12. https://doi.org/10.1016/j.eng.2021.12.006

Livingston, Edward, Angel Desai, and Michael Berkwits. 2020. "Sourcing personal protective equipment during the COVID-19 pandemic." *Jama* 323 (19): 1912-1914. https://doi.org/10.1001/jama.2020.5317

MacCarthy, Bart L, Wafaa AH Ahmed, and Guven Demirel. 2022. "Mapping the supply chain: Why, what and how?" *International Journal of Production Economics* 250: 108688. https://doi.org/10.1016/j.ijpe.2022.108688

Marucheck, Ann, Noel Greis, Carlos Mena, and Linning Cai. 2011. "Product safety and security in the global supply chain: Issues, challenges and research

opportunities." *Journal of Operations Management* 29 (7-8): 707-720. https://doi.org/10.1016/j.jom.2011.06.007

Mattox, Elizabeth. 2012. "Medical devices and patient safety." *Critical care nurse* 32 (4): 60. https://doi.org/10.4037/ccn2012925

Medical Plastic News. 2022. "Overcoming supply chain disruptions in medical device manufacturing." https://www.medicalplasticsnews.com/medical-plastics-industry-insights/medical-plastics-insights/overcoming-supply-chain-disruptions-in-medical-device-manufa/.

Miller, Fiona A, Steven B Young, Mark Dobrow, and Kaveh G Shojania. 2021. "Vulnerability of the medical product supply chain: the wake-up call of COVID-19." *BMJ Quality & Safety* 30 (4): 331-335. https://doi.org/10.1136/bmjqs-2020-012133

Mori, Marcella, Raffaella Ravinetto, and Jan Jacobs. 2011. "Quality of medical devices and in vitro diagnostics in resource-limited settings." *Tropical Medicine & International Health* 16 (11): 1439-1449. https://doi.org/10.1111/j.1365-3156.2011.02852.x

Muthuppalaniappan, Menaka, and Kerrie Stevenson. 2021. "Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health." *International Journal for Quality in Health Care* 33 (1): mzaa117. https://doi.org/10.1093/intqhc/mzaa117

Offices of The United States Attorneys. 2012. "Fifth New Jersey Health Care Practitioner Pleads Guilty in Cash-For-Patients Scheme." https://www.justice.gov/archive/usao/nj/Press/files/Patel,%20Dinesh%20Plea%20News%20Release.html.

Ozdemir, Dilek, Mahak Sharma, Amandeep Dhir, and Tugrul Daim. 2022. "Supply chain resilience during the COVID-19 pandemic." *Technology in Society* 68: 101847. https://doi.org/10.1016/j.techsoc.2021.101847

Pederson, Amanda. 2022. "Should Medtech get first dibs on semiconductors?" https://www.mddionline.com/components/should-medtech-get-first-dibs-semiconductors

Polisena, Julie, Jeffrey Jutai, and Rana Chreyh. 2014. "A proposed framework to improve the safety of medical devices in a Canadian hospital context." *Medical Devices: Evidence and Research*: 139-147. https://doi.org/10.2147/MDER.S61728

Pranggono, Bernardi, and Abdullahi Arabo. 2021. "COVID-19 pandemic cybersecurity issues." *Internet Technology Letters* 4 (2): e247. https://doi.org/10.1002/itl2.247

Rangel, Djalma Araújo, Taiane Kamel de Oliveira, and Maria Silene Alexandre Leite. 2015. "Supply chain risk classification: discussion and proposal." *International Journal of Production Research* 53 (22): 6868-6887. https://doi.org/10.1080/00207543.2014.910620

Rebecca Pifer. 2021. "More than 1/3 of health organizations hit by ransomware last year, report finds." https://www.healthcaredive.com/news/more-than-13-of-health-organizations-hit-by-ransomware-last-year-report-f/602329/.

Rudolf, Paul M, and Ilisa BG Bernstein. 2004. "Counterfeit drugs." *New England Journal of Medicine* 350 (14): 1384-1386. https://doi.org/10.1056/NEJMp038231

Sametinger, Johannes, Jerzy Rozenblit, Roman Lysecky, and Peter Ott. 2015. "Security challenges for medical devices." *Communications of the ACM* 58 (4): 74-82. https://doi.org/10.1145/2667218

Semiconductor Industry Association. 2020. *From Microchips to Medical Devices: Semiconductors as an Essential Industry during the COVID-19 Pandemic.* *https://www.semiconductors.org/wp-content/uploads/2020/10/From-Microchips-to-Medical-Devices-SIA-White-Paper.pdf*

Semiconductor Industry Association. 2021. "Semiconductors are the Brains of Modern Electronics." https://www.semiconductors.org/semiconductors-101/what-is-a-semiconductor/.

Senna, Pedro, Augusto Reis, Igor Leão Santos, Ana Claudia Dias, and Ormeu Coelho. 2020. "A systematic literature review on supply chain risk management: is healthcare management a forsaken research field?" *Benchmarking: An International Journal* 28 (3): 926-956. https://doi.org/10.1108/BIJ-05-2020-0266

SenseOn. 2023. "How Much Should A Business Spend on Cybersecurity." https://www.linkedin.com/pulse/how-much-should-business-spend-cybersecurity-senseon-tech/

Sheffi, Yossi. 2015. "Preparing for disruptions through early detection." *MIT Sloan Management Review* 57 (1): 31. https://sloanreview.mit.edu/article/preparing-for-disruptions-through-early-detection/

Shen, Bin, Ming Cheng, Ciwei Dong, and Yixuan Xiao. 2021. "Battling counterfeit masks during the COVID-19 outbreak: quality inspection vs. blockchain adoption." *International Journal of Production Research*: 1-17. https://doi.org/10.1080/00207543.2021.1961038

Sridharan, Kannan, and Gowri Sivaramakrishnan. 2023. "Disinformation about COVID-19 preventions and treatments: analysis of USFDA warning letters." *Health Communication* 38 (5): 885-891.

https://doi.org/10.1080/10410236.2021.1980254

Tang, Christopher S. 2006. "Robust strategies for mitigating supply chain disruptions." *International Journal of Logistics: Research and Applications* 9 (1): 33-45. https://doi.org/10.1080/13675560500405584

The Covid Crisis Group. 2023. *Lessons from the Covid War: An Investigative Report*. PublicAffairs.

The White House. 2022. "Fact Sheet: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China." https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/.

Thimbleby, Harold. 2013. "Improving safety in medical devices and systems." 2013 IEEE International Conference on Healthcare Informatics. https://doi.org/10.1109/ICHI.2013.91

Tomlin, Brian, and Yimin Wang. 2011. "Operational strategies for managing supply chain disruption risk." *The Handbook of Integrated Risk Management in Global Supply Chains*: 79-101. https://doi.org/10.1002/9781118115800.ch4

UBS. 2021. "Medical device sales recovering from COVID-19 disruption." https://www.ubs.com/global/en/wealth-management/our-approach/marketnews/article.1536314.html.

Uzsoy, Reha. 2005. "Supply-chain management and health care delivery: Pursuing a system-level understanding." *Building a Better Delivery System: A New Engineering/Health Care Partnership*: 143-146. https://doi.org/10.17226/11378

Van Norman, G. A. 2016. Drugs and Devices: Comparison of European and US Approval Processes. JACC: Basic to Translational Science, 1(5), 399-412. https://doi.org/10.1016/j.jacbts.2016.06.003

Vockley, Martha. 2016. "The servicing of medical devices: in need of repair, regulation, or redemption?" *Biomedical Instrumentation & Technology* 50 (5): 316-328. https://doi.org/10.2345/0899-8205-50.5.316

Walker-Roberts, Steven, Mohammad Hammoudeh, and Ali Dehghantanha. 2018. "A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure." *IEEE Access* 6: 25167-25177. https://doi.org/10.1109/ACCESS.2018.2817560

Weiner, Stacy. 2021. "The growing threat of ransomware attacks on hospitals." https://www.aamc.org/news-insights/growing-threat-ransomware-attacks-hospitals.

World Health Organization (WHO). 1999. *Counterfeit drugs: guidelines for the development of measures to combat counterfeit drugs.* World Health Organization.

WHO. 2017. "WHO Global Model Regulatory Framework for Medical Devices including in vitro diagnostic medical devices." https://www.who.int/publications/i/item/9789241512350

WHO. 2020. *Coronavirus Disease 2019 (COVID-19): Situation Report, 73. https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200402-sitrep-73-covid-19.pdf*

Xu, Zhitao, Adel Elomri, Laoucine Kerbache, and Abdelfatteh El Omri. 2020. "Impacts of COVID-19 on global supply chains: Facts and perspectives." *IEEE Engineering Management Review* 48 (3): 153-166. https://doi.org/10.1109/EMR.2020.3018420

Aman Goswami is a 4th year PhD candidate at Rutgers University in the Supply Chain Management department. He is a supply chain and operations management researcher, with an interest in empirical research in healthcare operations. Previously, he worked in the industry as a data science manager, solving varied business problems in consulting and analytical domains for close to a decade. He plans to pursue an academic career with a strong interest in research, teaching, service, and leveraging his data science, consulting, and analytical industry experience to make scientific research more accessible and understandable.

Alok Baveja is a Professor of Supply Chain Management at Rutgers University. His expertise is in the use of innovative modeling and technologies for managing operations in public and private sectors. His research has appeared in numerous journals such as *Mathematics of Operations Research, IEEE Transactions on SMC, European Journal of Operational Research, California Management Review,* including a bestseller reprint in the *Harvard Business School's case series.* His research has been funded by grants from the National Science Foundation, the National Institute of Justice, U.S. Department of Transportation, The British Council, and Centers for Disease Control/New Jersey Department of Health.

Benjamin Melamed is a Distinguished Professor of Supply Chain Management at Rutgers University. His

research interests include supply chain management, supply chain financial management, service chain management (including modeling, analysis, simulation, and optimization), general systems modeling and performance evaluation, stochastic processes, traditional and hybrid simulation, and decision support tools. He has authored or co-authored over 120 papers, co-authored two books, and has published in a broad range of scientific journals, including *Operations Research, Mathematics of Operations Research, Management Science, J. of Applied Probability, and Annals of Operations Research*. He became AT&T Fellow in 1988 and IEEE Fellow in 1994.

Fred Roberts is the Director of the Department of Homeland Security University Center of Excellence CCICADA: Command, Control and Interoperability Center for Advanced Data Analysis, Director Emeritus of DIMACS: Center for Discrete Mathematics and Theoretical Computer Science, and Distinguished Professor of Mathematics at Rutgers University. His research interests include mathematical models in the social, behavioral, biological, epidemiological, and environmental sciences; theory of measurement; and homeland security issues of stadium security, transportation security, natural disasters, maritime cyber security, supply chain disruptions, and global environmental change. He has authored 5 books, edited 26 books, and authored over 215 papers.

Acknowledgements
This project has been funded in whole or in part with Federal funds from the Department of Homeland Security under BOA No. 70RSAT18G000000001, task order no. 70RSAT21FR00000127. The content of this publication does not necessarily reflect the views or policies of the Department of Homeland Security, nor does mention of trade names, commercial products, or organizations imply endorsement by the USA Government.