# Enterprise Network Models for Counterfeit Part Supply Chains Workshop
# August 5, 2021

University of Maryland

Funding for this project was provided by the National Science Foundation Division of Civil, Mechanical and Manufacturing Innovation (Grant No. CMMI2039958)

# Enterprise Network Models for Counterfeit Part Supply Chains Workshop

Counterfeit electronic products have been a reality for many years. Nearly all of the treatment of this problem to date has focused on the detection of counterfeits, which is necessary, but a purely defensive step. Without a network model of the supply chain, disruptions can be haphazard and inadequately targeted.

A network model that includes business strategies of distributors of obsolete parts, the ability of laboratories to detect counterfeit parts, impacts of buyback, and return policies is needed. The implications of enforcement (e.g., administrative, legal, or reputational) of anti-counterfeiting policies and the levels of penalties for supplying and accepting counterfeit parts also need to be accommodated in network models.

The objective of the workshop is to examine enterprise network modeling as a tool for understanding and disrupting counterfeit electronics supply chains. Participants in the workshop included electronics supply-chain members from OCMs to users, supply-chain monitoring technology developers, academics, policymakers, legal and law enforcement, and other stakeholders.

**Workshop Details**
The virtual Workshop was held on August 5, 2021, via ZoomGov. The workshop included the following six sessions:

- Introduction
- Counterfeit Electronics Supply Chain
- Traceability, Tracking, and Transparency
- Policies – Standards, Legal Acquisition, Law Enforcement
- Network Modeling
- Wrap Up

The workshop had 125 "unique" participants. The workshop was recorded to assist in the production of this report (the recording is destroyed after the preparation).

**Organization of this Document**
This document provides an overall workshop summary followed by summaries of the individual panels. This document follows the Chatham House Rule with redaction of individual names and organizational identifications.

# Workshop Summary and Outlook

**Diganta Das, Hirbod Akhavantaheri, Peter Sandborn (UMD Engineering)**

Despite a substantial body of work focused on developing detection methodologies and detection enabling technologies, relatively little attention has been paid to modeling the networks responsible for creating and distributing counterfeit parts for critical systems. This workshop focused on how one could create an enterprise network model for the electronic part counterfeit supply chain. The objective of such a model is to capture all the participants in the supply chain and their connections. The resulting model could be used to assess the risk of various supply-chain disruptions and other relevant supply-chain events culminating in a quantification of the counterfeit risk to the final customer. The network model could also be used to assess the "value" of mitigation, the efficacy of tracking and disruption actions, including the application of policies.

Network Modeling

The basis of network analysis is that individual nodes are connected by relationships that form networks. Network analysis is well suited to the study of supply chains since they consist of networks of individuals and groups that span geography, political entities, economic status, and social ideologies.[1]

Socio-technical systems are defined as systems that involve both complex physical-technical systems and networks of interdependent actors. In general, system behavior can be analyzed (and improved or disrupted) only by considering both social and technical sub-systems and their interdependencies. In other words, the structure and behavior of both social and technical sub-systems give rise to the overall behavior of a socio-technical system.

Socio-technical systems involve behavioral and social aspects of people and society that interact with technical aspects of organizational structure and processes -- both engineered and natural -- to create organizational outcomes and overall system performance. These types of systems are often characterized as complex adaptive systems where independent agents pursue their individual objectives while learning and adapting to evolving system structures and behaviors.

An agent-based model (ABM) is a computational model for simulating the actions and interactions of autonomous agents (both individual or collective entities) to understand the behavior of a system and what governs its outcomes. It combines elements of game theory, complex systems, emergence, computational sociology, multi-agent systems, and evolutionary programming. Monte Carlo methods are used to understand the stochasticity of these models. Generally, agent-based models are composed of: (1) numerous agents specified at various scales; (2) decision-making heuristics; (3) learning rules or adaptive processes; (4) an interaction topology; and (5) an environment.

Agent-based models can be embedded within a system dynamics-based simulation to model a network's evolution in time. For application to counterfeit supply chains, the system dynamics simulation models the causal loops associated with the supply and demand for parts.

The Counterfeit Parts Supply Chain Network

In this workshop, we discussed the use of network modeling to provide a better understanding of the electronics supply chain. For the counterfeit parts supply chain, the network is a combination of technical interactions (facilities, detection capability, and flows of parts and money) and social interactions (procurement decisions and risk tolerance) because you can't model the counterfeit network without considering the technology, people and the prevailing business environment.

[1] We are using the term "supply chain", but inherently supply chains have a graph or network structure. They are not generally hierarchical or one-to-one, but rather interconnected and involving multiple levels; there may also be no clear way to distinguish the tiers of the supply chain.

Who are the Agents?

A fundamental question addressed in this workshop is who are the agents, i.e., what entities are relevant to the supply chain for counterfeit parts? The following is a high-level list of possible agents. Note, not all of these agents necessarily always play an integral role in the network depending on policies and other constraints that are in play. Participation of the agents depends on the nature of the transaction

- Customers
- Original Component Manufacturers (OCMs)
- Authorized Distributors
- Independent Distributors
- Brokers
- Test Laboratories
- Law Enforcement
- Policy Makers
- End-of-Life Participants (e.g., recyclers, consignment handlers)

These stakeholders and their connections represent a network that defines the flow of parts, information, and financial transactions. Each stakeholder (agent) is described by a set of behaviors and goals (each has a potentially unique motivation). Together, the network and the independent behaviors/goals of the stakeholders define outcomes that translate into the risk (and timing) of compromised parts.

Possible Uses of the Network Model

An important question to ask is, how will the network be used to create value for stakeholders? The participants pointed out that network models can be useful for articulating (communicating) the problem to non-experts involved in making policies but who may lack the ability to detect unintended policy consequences. A network model can provide a platform to perform a "what-if" analysis for various possible scenarios. The network model needs to consider how it delivers value in the following ways:

- Identify patterns
  - What series of events can lead to counterfeit parts being sold or accepted
- Measure risk
  - What is the probability that a supply-chain disruption results in counterfeits?
  - What is the probability that counterfeits reach the customer?
- Predict timing
  - How long will it take for a supply-chain disruption to result in counterfeits (if it ever does), and how long will it take for those counterfeits to reach the customer?
- Test policy
  - What is the effectiveness of various policies on the risk and timing?
- Test technology adoption impacts
  - What is the impact of technology adoption on risk mitigation and cost?

# Counterfeit Electronics Supply Chain Panel

**Diganta Das (UMD Engineering), Robert Bodemuller (Lockheed Martin)**

This panel addressed the following questions and topics:

- What unlikely but possible scenarios need to be covered by the model (i.e., black swan events)
- How do authorized distributors choose whom to sell to when there are multiple demands and limited inventory (e.g., independent distributors vs. Prime contractors)?
- How do distributors or customers approach the purchase of components slated for obsolescence?
- How do you determine the risk of counterfeit to decide whether testing is needed? If testing is needed, how is the level of testing decided upon?
- What are the ideal inputs and outputs of the model? Where in the model do you want to probe for information?

The critical points developed in this panel included:

- Black swan event examples –Suez canal blockage, Taiwan in a conflict, pandemics, broadly, any trends that reduce part availability.
- Raw material supply to the foundries can affect the entire supply chain (factory fire in Japan, for example).
- Modeling the effects of events in part availability is critical.
- Beyond direct costs and calculations, decisions to do business in shortage time depend on relationships. In addition, one does consider the revenue impact, global use for the entire company, and the customer's ability to pay.
- Independent distributors follow proprietary purchasing strategies based on public information and data from their customers and suppliers.
- Purchase of obsolete parts by independent distributors can be speculative since one can always sell off unsold excess inventory. Unfortunately, there is a possibility that suspect actors from around the globe can buy such excess inventory, and those can become raw materials to make counterfeit parts.
- Independent distributors are not constrained by OCM contracts constraining them on customers, lot size, pricing, or geographic areas compared to authorized distributors. That's why they can act quickly to market changes and fill an essential role in the supply chain.
- The money trail may not lead to counterfeit activity – as some members of the supply chain would finally buy from some legitimate source for material, for example.
- The need for testing should be risk-based – supplier, application, part type (people came to the AS 6171 factors independently).
- Be careful whom you buy from – why would a random company have a part when other big guys do not.
- Purchasing from authorized distributors or established independent distributors does not warrant testing. However, periodic audits are necessary even for complying partners.
- Wire frauds are becoming a bigger problem than counterfeiting.
- Counterfeiting of test reports must be treated as seriously as counterfeit parts.
- Check everything – who are they, where, how long in business, certification, google map (consistency in CAGE code and DUNS number addresses).
- Because of their caution, good independent distributors may have good practices that are worth learning from.

- Escrowing the payment for parts is coming back (was not allowed by law for a time?). Escrowing payment is a deterrent for some types of counterfeit part transactions. The network model needs to model escrow.

# Summary of the Traceability, Tracking, and Transparency Panel

**Diganta Das (UMD Engineering), Michael Ford (Aegis Software)**

This panel addressed the following questions and topics:

- What motivates companies to participate in an industry-wide tracking and traceability activity?
- How is the value of information sharing determined and weighed against counterfeit risk and interest of protecting business information?
- In the transactions and through the supply chain, what should be tracked and what can be tracked?
- How are the "value" and "effectiveness" of distributed ledgers quantified? How are the technologies verified before implementation?
- Can a track and trace system survive changes in items such as technology, company ownership, and law regarding data retention?

The essential points developed in this panel included:

- A complete system needs to be software-based, machine-recorded, and machine-shared data sharing for internal and external traceability.
- The weak points in a supply chain can be isolated and neutered if not eliminated.
- Have to have a combination of internal and external traceability.
- Currently, in the absence of tracking and tacking, counterfeiters have significantly higher benefits than their cost. The supply chain members have to be convinced of the benefits, and the benefits have to span beyond counterfeit and need to show how it helps with trust, liability reduction, and brand protection. One can also show that the speed of business can improve through the adoption of tracing and tracking
- The appropriate cost of such technologies is driven by the cost of purchasing or selling counterfeit parts. Once the cost of that technology goes below that threshold, supply chain adoption is more likely.
- It cannot be assumed that the majority of the supply chain will adopt these technologies. However, some entities in the supply chain will adopt them and provide unique services within the supply chain.
- With a blockchain – you will know if somebody tampered with the data; however, do not expect it to work like magic.
- Tracing technologies allows stakeholders to identify the entity responsible for introducing the part in the supply chain. They do not prevent or treat the problem.
- If there is a gap in the part traceability, its validity is lost at the gap.
- The required human input in IPC 1782A and 1783 is a vulnerability for the standard. That's why IPC CFX was developed to automate the process. As long as people are responsible for inputting data in the ledger, traceability technologies cannot be considered fully secure.
- With a public blockchain, when a company departs the market, it does not matter.
- The data size is overwhelming – how much is needed, and how much are you prepared to store in a secure environment. Who will pay for this – storage of data – can we trust one person?
- Limit data sharing to "have I seen it before" without giving the details of the product. Process traceability can help reduce product traceability data by moving the trust to the process that produced it.

- Credentials are like a college degree – you do not need to publish all of the transcripts to prove that you have achieved a level of knowledge.

# Summary of the Policies – Standards, Legal Acquisition, Law Enforcement Panel

**William Lucyshyn (UMD Public Policy), Bill GreenWalt (American Enterprise Institute)**

This panel addressed the following questions and topics:

Considerations that make this hard:

- Technology trends – commercial moves faster than defense
- Globalization of commercial supply chains
- Outsourcing to China
- The end of the cold war leading to a decline in defense spending and subsequently keeping equipment in operation longer
- Shift from just-in-case to just-in-time inventory management
- The complexity of supply chains (lost visibility, agency and control)

The panel discussed the following:

- Introduced the major trends impacting the global industrial trends.
- Reviewed the policy framework io include laws, regulations, agency policies, and industry standards.
- Summarized the congressional considerations for development of the counterfeit policies.
  - Data was a challenge, and as a result anecdotal info was used to inform the debate.
- The changes led to making contractor purchasing systems compliant – these are reviewed every 3 years.
- Contractors were now also required to flow down the counterfeit requirements to all of their subcontractors required to have government compliant cost accounting systems (CAS).
- However, there is a reluctance of government to enforce, putting the onus on contractor.
- Recommendations included:
  - This is a whole of the economy issue, since government acquisition is a small customer in the commercial marketplace.
  - Success does not mean all critical capabilities must be produced onshore—it's not a realistic solution.
  - Consider developing a better industry framework with trusted partners, and reinvigorate the trusted foundry program.
  - Clean up all the policy framework to make policies and definitions consistent.

# Summary of the Network Modeling Panel

**Peter Sandborn, Hirbod Akhavantaheri (UMD Engineering), Douglas Bodner (Georgia Tech)**

This panel has three distinct discussions: general systems-of-systems modeling, previous issues/challenges encountered when network modeling counterfeit part supply chains, and possible future directions for network modeling.

System-of-Systems (SoS) Modeling:

The problem addressed in this workshop is a system-of-systems (SoS) problem. SoS problems are characterized as:

- Operational independence of component systems
- Managerial independence of component systems
- Geographically distributed
- Evolutionary development processes
- Emergent behavior

The specific challenges modeling (managing) SoS are that nobody is in charge, the capabilities of constituents (the component systems) are complex and maybe unknown (including behavior and motivations), validating and learning, the autonomy of component system, and the emergent behavior that can take place.

Specifically, the type of SoS in our case is a "collaborative" in which the component systems interact voluntarily to fulfill an agreed-upon central purpose. Collaborative SoS have organizations and groups as constituents; they are not engineered (nobody planned the network), evolution is based on the dynamic interactions among constituents (building and eroding of trust fits in this category), individuals make changes based on local objectives and interactions with others, and changes in one constituent can affect actions of others.

Network Modeling Challenges:

Building a network model is challenging, but also implementing/executing the model in a practical way that allows the generation of useful result may be more difficult, i.e., for large SoS, modeling is very cumbersome. Judiciously breaking top-level models into smaller parts ("snippets") on which analysis tools can be used was suggested. Additional modeling challenges experienced by others include:

- Previous simulations were good for articulating (communicating) the problem to non-experts, but the work did not seem to be very useful for detecting unintended policy consequences.
- Adaptive behavior has to be captured (counterfeiters adapt, the policy has to adapt too).
- Policy changes will restructure the supply chain, i.e., change the network, meaning that there is no single network model.
- There may be a need for a model down to individual systems to generate the sort of results stakeholders want.
- Traditional validation approaches may be counterproductive. If you only collect data from SMEs then you get back exactly what the SMEs expected.
- If agents are really constrained, their behavior is easy to model; if they are not constrained, it is tough to model their behavior.
- Agent objectives and connections need to be dynamic. If agents are constrained by a set goal and predetermined connections, no unexpected pattern will emerge.

- How do we know if we have the right agents connected in the right way? This is a big risk (we only model what we know about), continuous validation by using the model on lots of scenarios.
- What policies are bad doesn't necessarily shed light on which ones are good.

Network Modeling Opportunities:

- Exploratory instead of consolidative modeling (Bankes, 1993).
- Employ a family of smaller models (snippets).
- Validate pieces rather than the whole.
- Intentionally explore conflicting or counterfactual assumptions.
- What about refreshing systems that parts go into faster, does that solve the problem (i.e., not a policy solution, but may be a solution that can be addressed by network models)?
- Solutions have to be robust (provide usable solutions when there is lots of uncertainty).