Additive Manufacturing Security – Research Field Overview

Commonwealth Scientific and Industrial Research Organisation (CSIRO)
April 4, 2024

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)

AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING

Affiliated

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

Part 1 ø ;)
Additive Manufacturing (AM)

Sci-Fi Vision

"But this constructor is both efficient and flexible. I feed magnetronic plastics — the stuff they make houses and ships of nowadays — into this moving arm. It makes drawings in the air following drawings it scans with photo-cells. But plastic comes out of the end of the drawing arm and hardens as it comes. This thing will start at one end of a ship or a house and build it complete to the other end, following drawings only."

– Murray Leinster, Things Pass By, 1945

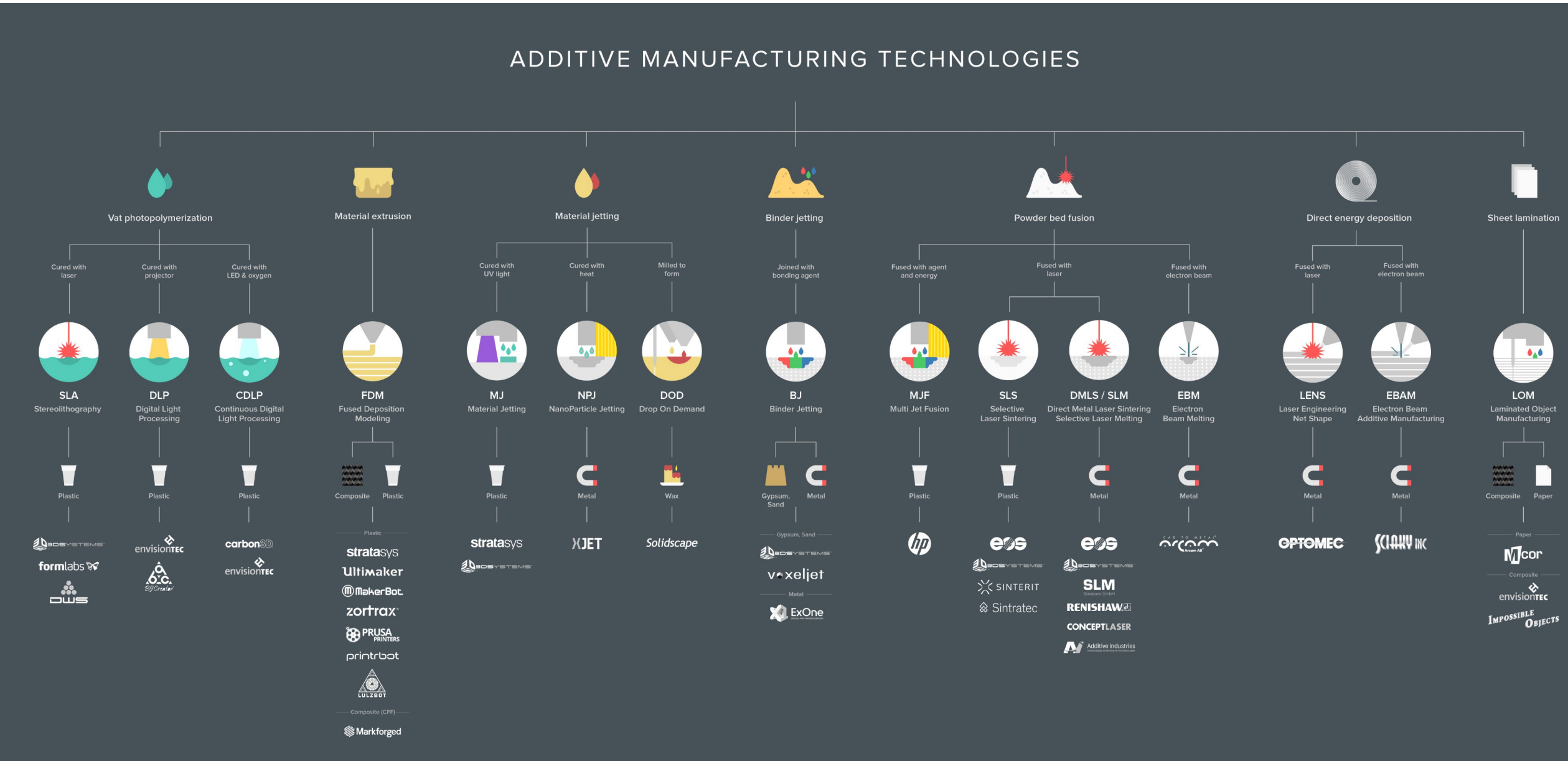
Designation: F2792 – 12a

Standard Terminology for
Additive Manufacturing Technologies[1,2]

Additive Manufacturing (3D Printing)

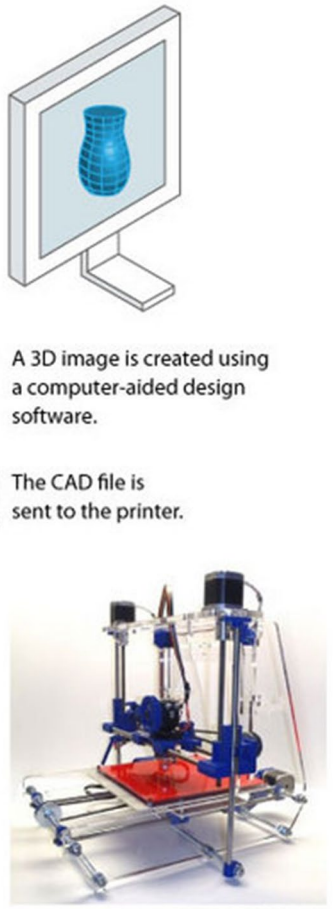
"additive manufacturing (AM), n — a process of joining materials to make objects from 3D model data, usually layer upon layer, as opposed to subtractive manufacturing methodologies."

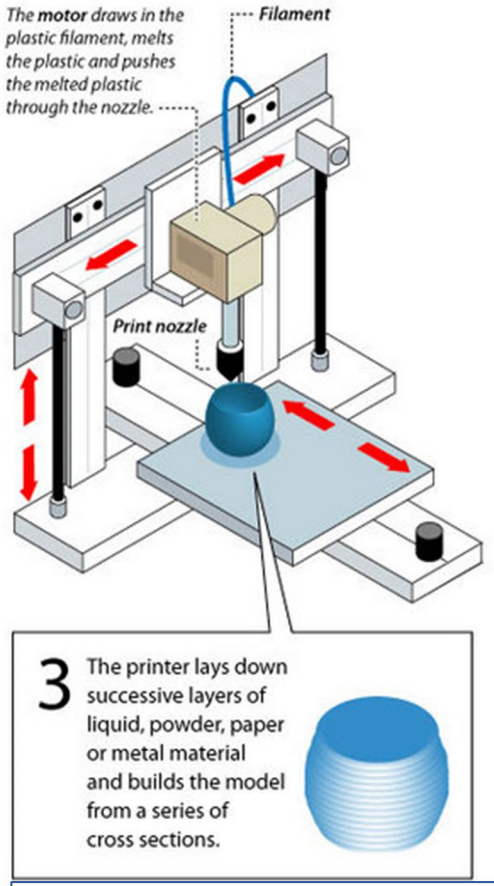
Many Modalities of AM



Fused Deposition Modeling (FDM)

- "Material Extrusion, n—an additive manufacturing process in which material is selectively dispensed through a nozzle or orifice."
  - "Fused Deposition Modeling (FDM), n—a material extrusion process used to make thermoplastic parts through heated extrusion and deposition of materials layer by layer; term denotes machines built by Stratasys, Inc."





ASTM International, F2792 – 12a "Additive Manufacturing Technologies"

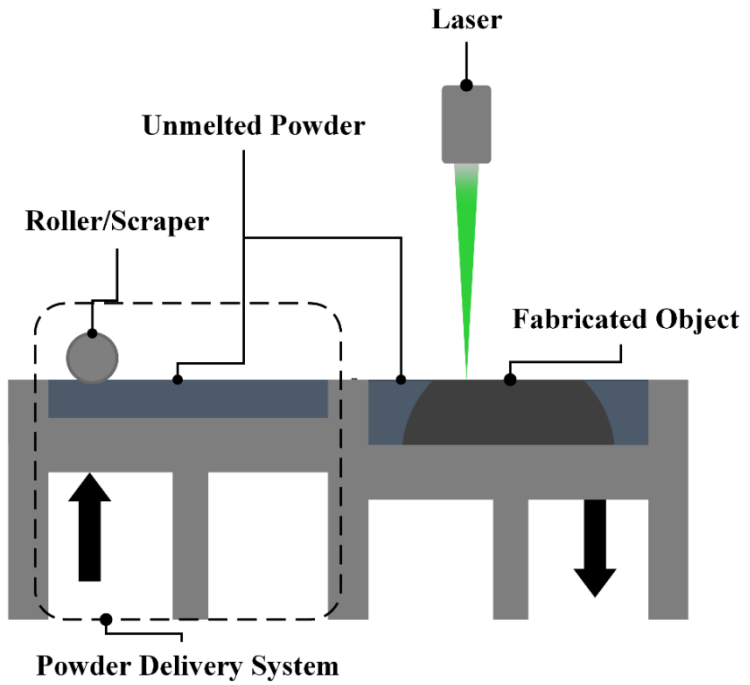
Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

Powder Bed Fusion (PBF)

- "Powder Bed Fusion, n—an additive manufacturing process in which thermal energy selectively fuses regions of a powder bed."
  - "*Focused thermal energy* means that an energy source (e.g., laser, electron beam, or plasma arc) is focused to melt the materials being deposited"

ASTM International, F2792 – 12a "Additive Manufacturing Technologies"

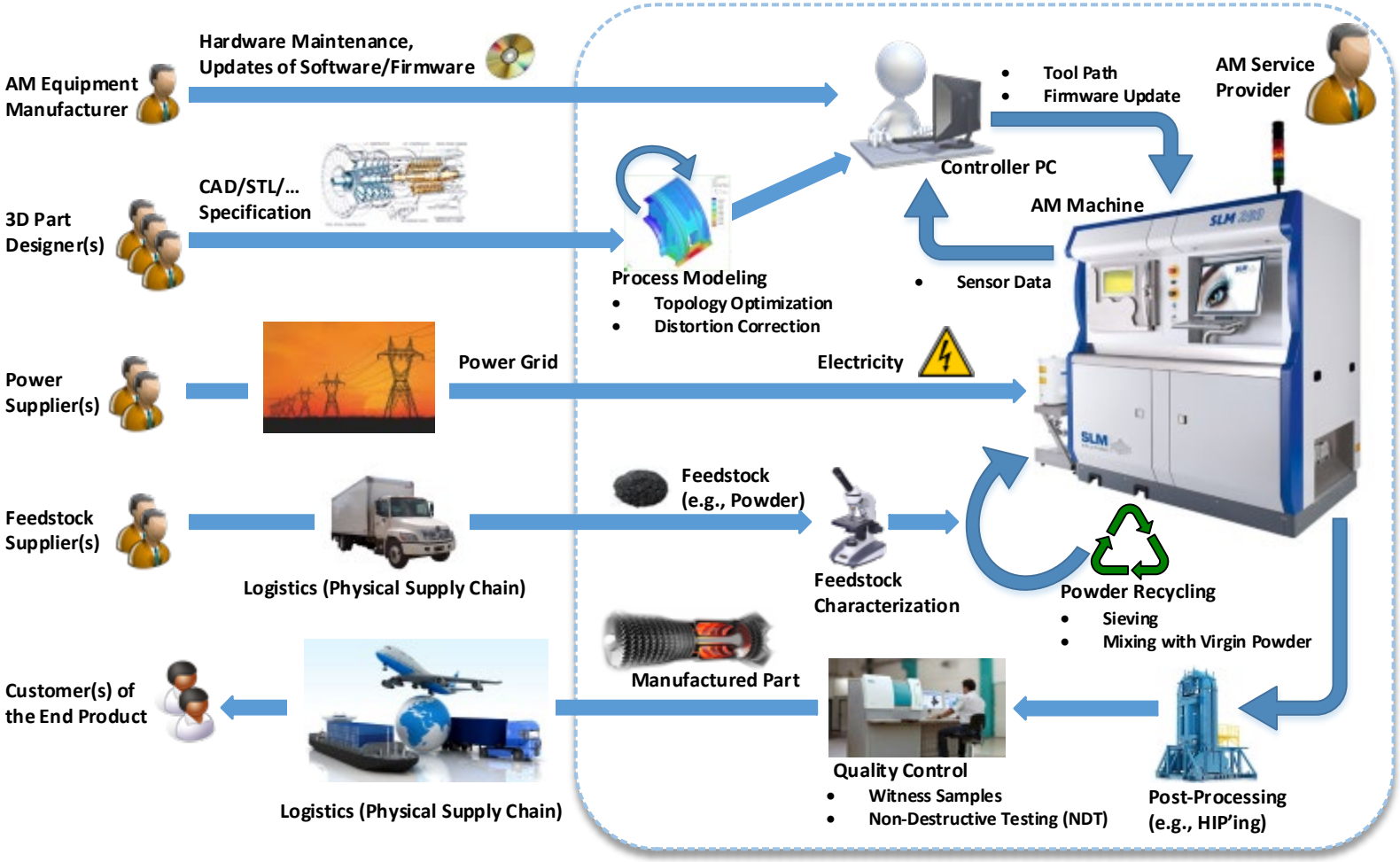


Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

AM is *not just* a 3D Printer ;)

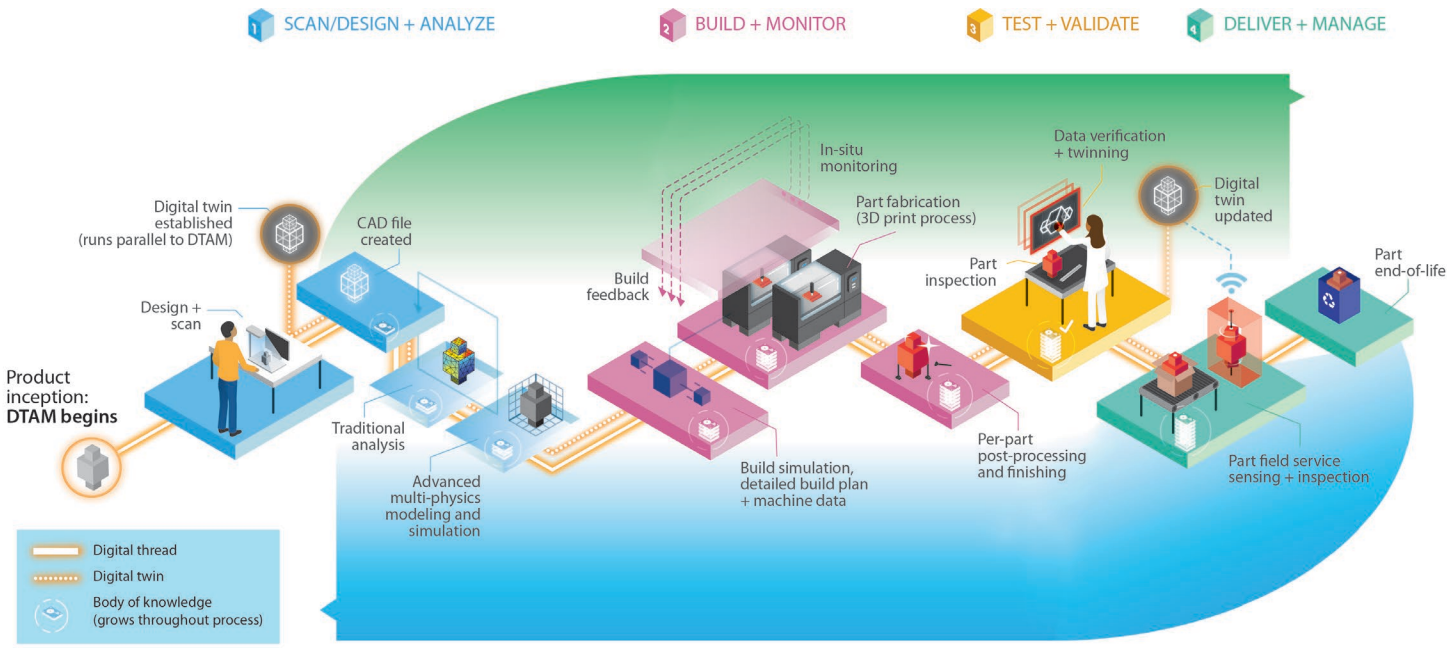
AM Workflow



Yampolskiy et al., "Security of Additive Manufacturing: Attack Taxonomy and Survey." Additive Manufacturing, vol. 21, pp. 431-457, 2018.

AM Digital Thread

Brown, J., Ezzard, J., Goldenberg, S., Haid, J., 2016. 3D opportunity and cyber risk management Additive manufacturing secures the thread,

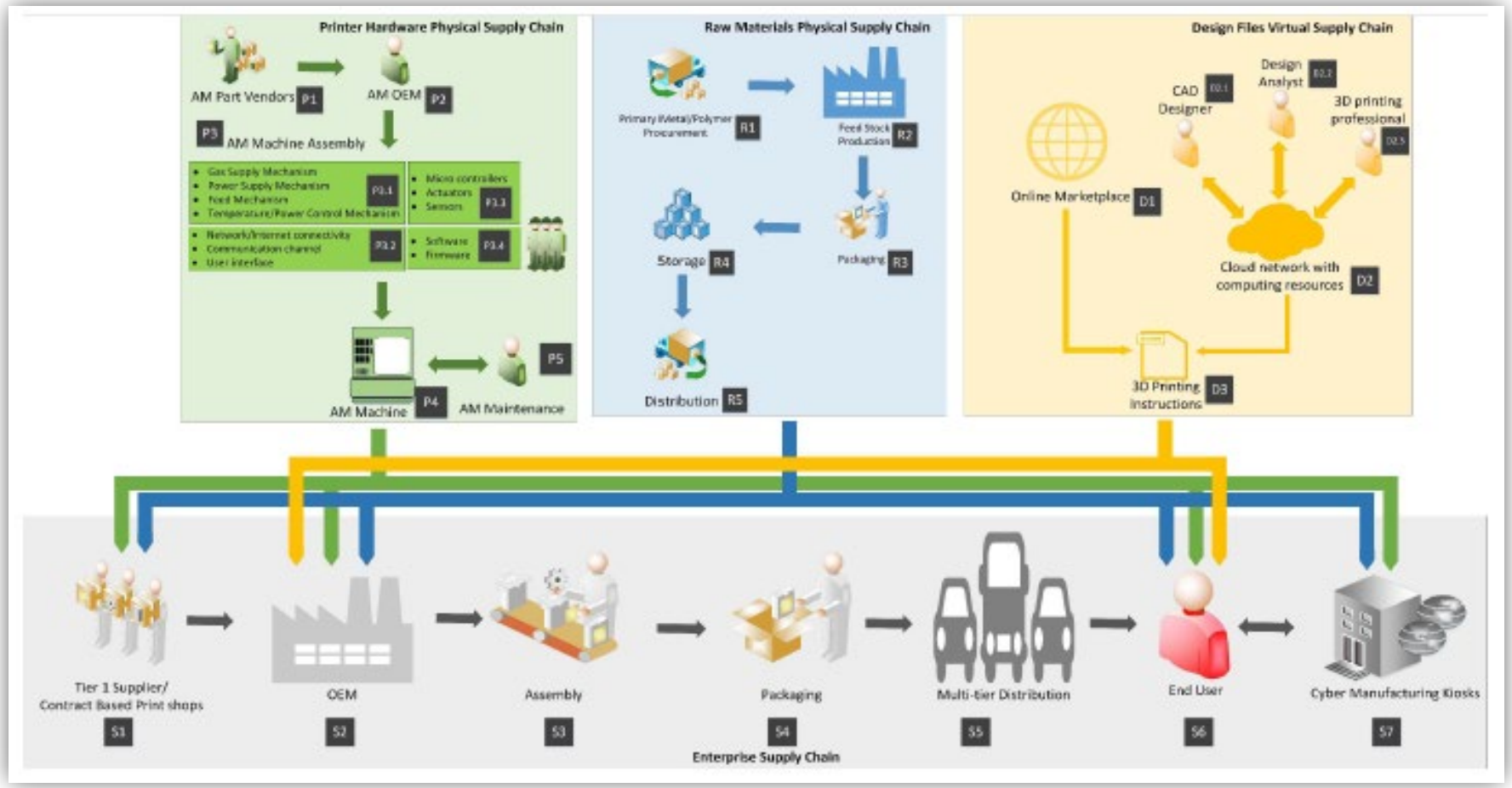


Today, significant tacit knowledge is required for success

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

AM in Supply Chain



Gupta et al., "Additive manufacturing cyber-physical system: Supply chain cybersecurity and risks." IEEE Access, vol. 8, pp. 47322-47333, 2020.

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

AM has numerous unique benefits

Advantages of AM (1)

Logistics

- Manufacturing of discontinued parts (e.g., based on 3D scan)
  - ⇒Sustainability of legacy equipment
- Just in time / on-demand manufacturing
  - ⇒Reduction of need for storage of spare parts
- In-place/proximity manufacturing
  - ⇒Reduction of transportation need

Part Performance

- Consolidation of parts
  - ⇒Reduced need for assembly
  - ⇒Increase part performance/ durability

https://www.additivemanufacturing.media/articles/optimize-additive-manufacturing-designs-for-cost-and-function

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

Advantages of AM (2)

DM/ML/AI-enabled

- Function-optimized parts
  - ⇒Reduced material use
    - ⇒ Reduced material waste
    - ⇒ Reduced costs per part
  - ⇒Reduced weight
    - ⇒ Increased fuel efficiency
- Process optimization
  - ⇒Detection of problems
  - ⇒Reduced number of failed builds
  - ⇒Reduced number of experimental parts for evaluation (coupons etc.)

https://www.additivemanufacturing.media/articles/optimize-additive-manufacturing-designs-for-cost-and-function

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING
- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

Staggering AM growth over past 30 years

Examples (few of many)

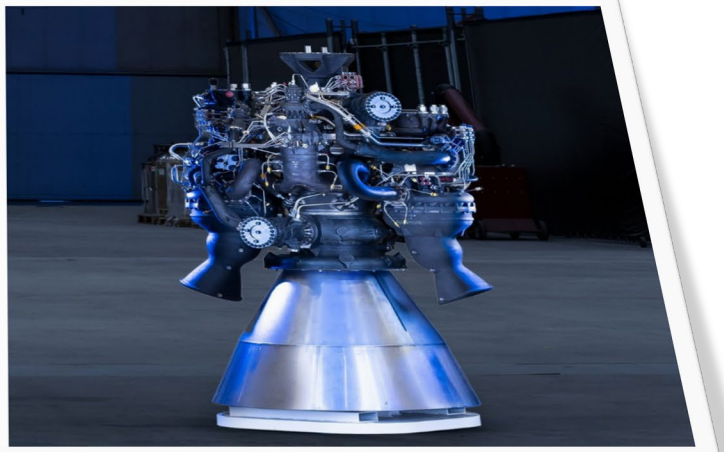
Aeon R Engine Development

ITERATIVE DEVELOPMENT FOR ENHANCED PERFORMANCE

Terran R utilizes our 3D printed Aeon R engines, an evolution of our Aeon 1 engines, to enable optimal propulsion. Leveraging proprietary 3D printing techniques, we are able to design more function into the engines, with less material, for less cost. Through our iterative development process, we have designed a single Aeon R engine to have 25% more thrust than all nine Aeon 1 engines combined.

STAGE 1

+ *13x 3D-printed Aeon R rocket engines*
+ *Aeon R sea level thrust of 258,000 lbf combined vehicle liftoff thrust of 3,354,000 lbf*



Aviation's manufacturing plant in Auburn, Alabama, celebrates its 30,000th 3D-printed fuel nozzle tip for the LEAP engine.

This week, the 30,000th additively-manufactured fuel nozzle tip "grew" on a 3D printer at GE Aviation's plant in Auburn, Ala., where the jet engine maker opened the industry's first site for mass production using the additive manufacturing process.

Online:

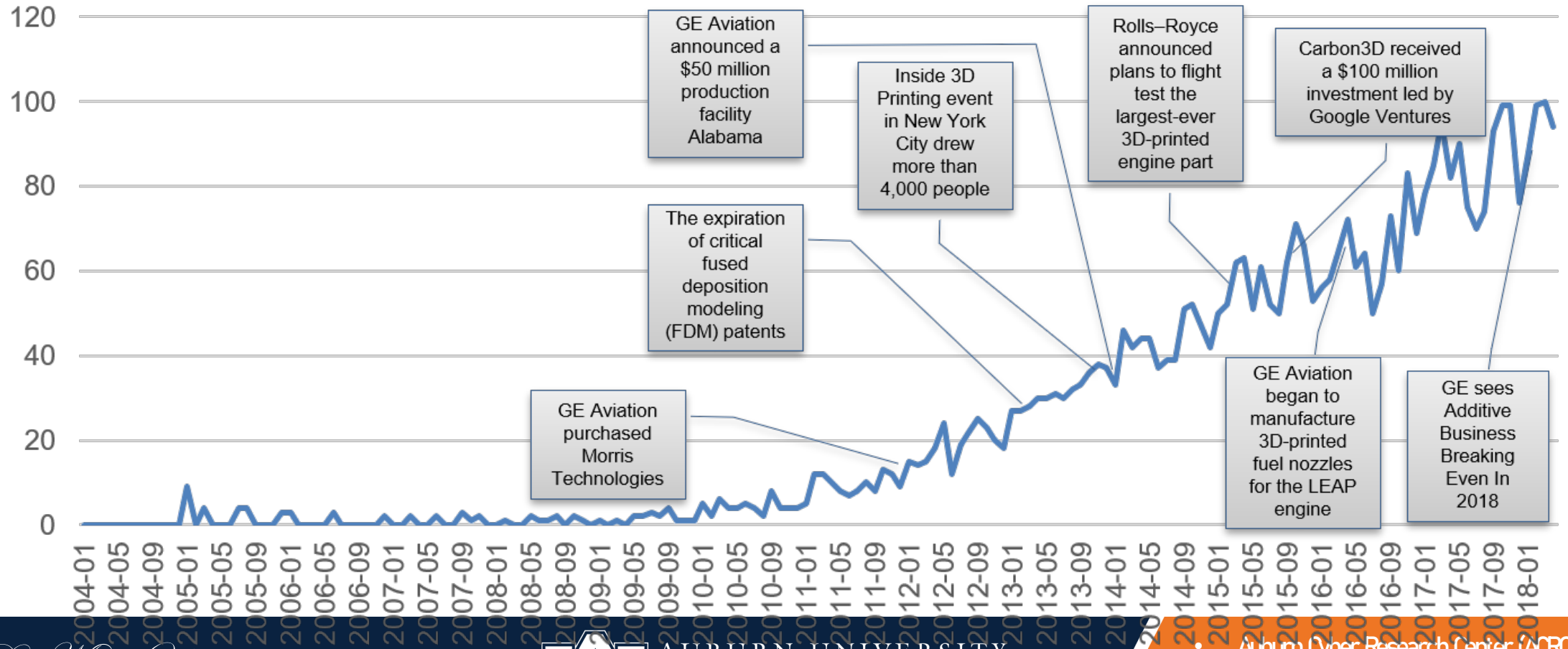
- https://www.ge.com/additive/stories/new-manufacturing-milestone-30000-additive-fuel-nozzles
- https://www.relativityspace.com/terran-r/#aeon-r

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)

AUBURN UNIVERSITY
SAMUEL GINN
COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

International Interest in AM

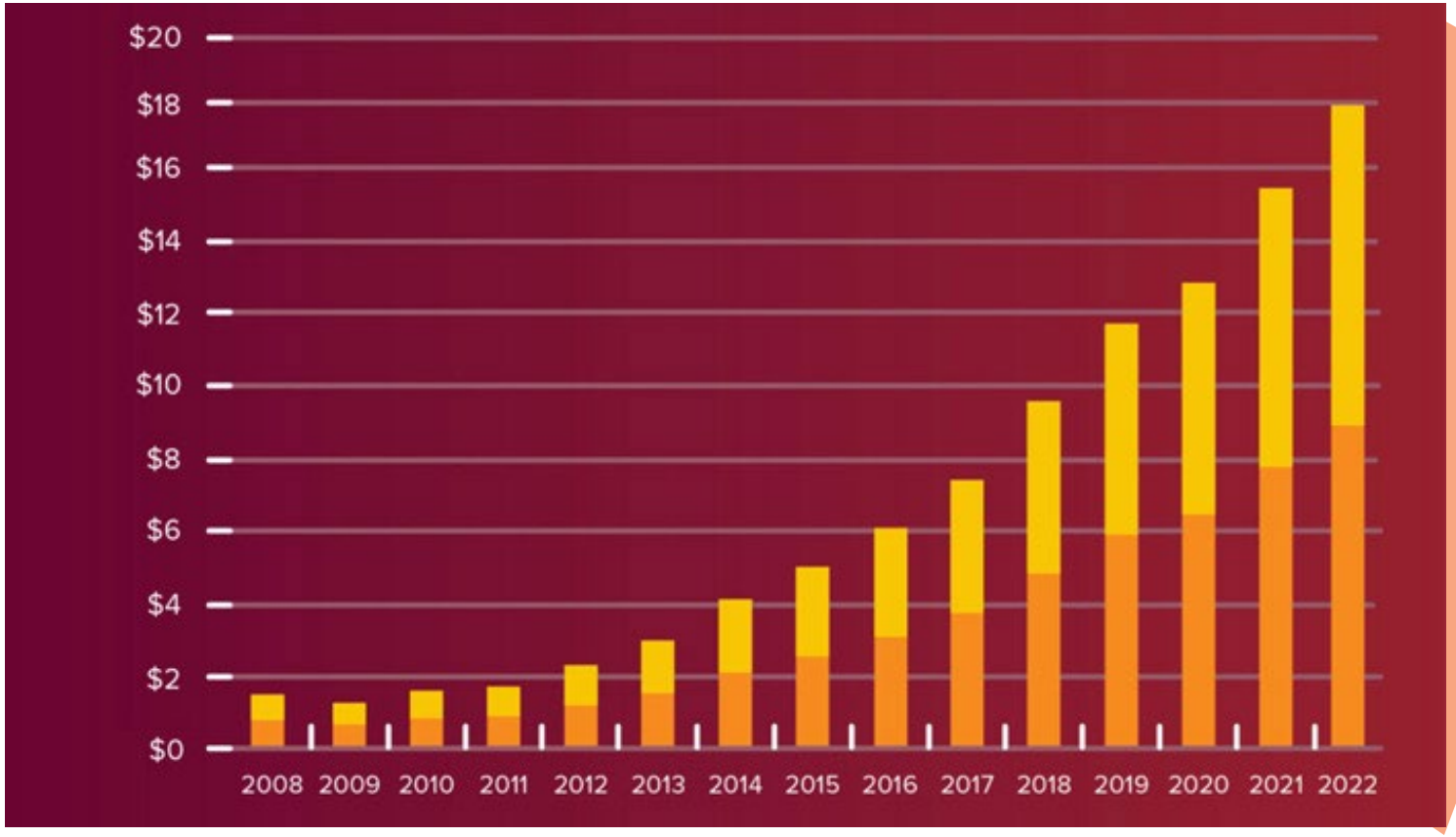


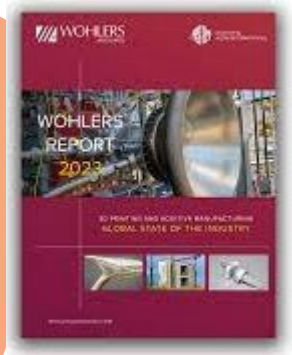
Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)

AUBURN UNIVERSITY
SAMUEL GINN
COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

Global Revenue for AM



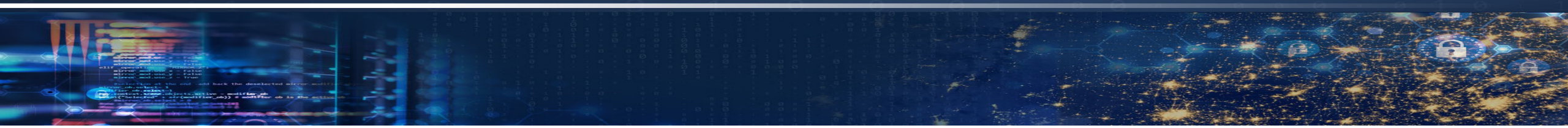


Global revenue for additive manufacturing services (yellow) and products (orange), expressed in billions of dollars

https://www.3dnatives.com/en/wohlers-report-2023-double-digit-growth-additive-manufacturing-030420235/#!

"The average annual growth rate of worldwide revenues produced by all products and services over the past 29 years is an impressive 26.6%."

- Wohlers Report



Part 1
AM-specific Security Threats

Do we need to Secure AM?

Manufacturing Industry in Hackers' Crosshair

A vibrant industrial base that can serve the country's critical needs during times of peace and war is a top national security matter. Manufacturers in the United States generated $6.0T in gross output in 2017, which represents 31% of the economy.[17] As manufacturers invest in digital manufactur-

investments are protected with a strong cybersecurity posture. Already, 35% of all cyber-espionage attacks in the U.S. are targeted at the manufacturing sector, the largest of any single sector.[18] Adoption of digital manufacturing technologies will increase the U.S. manufacturing sector's attack surface and simultaneously make it an even more attractive target as it becomes a key differentiator for building competitive economic advantage.

90% of U.S. manufactured GDP and yet have the most limited resources for protecting their operations. U.S. Manufacturing is highly fragmented with 98% of all manufacturers having 500 or fewer employees and 73% having 20 or fewer employees.[19] Many of these manufacturers lack resources with the necessary technical skills to adopt productivity-enhancing digital technologies in a way that responsibly protects them from cyber-attacks.

17 www.bea.gov
18 NDIA Cybersecurity for Manufacturing Networks (October 2017), www.ndia.org/-/media/sites/ndia/divisions/working-groups/cfam/ndia-cfam-2017-white-paper-20171023
19 www.nam.org/Newsroom/Facts-About-Manufacturing/

It is not a Matter of "if" but of "when" AM will be Attacked

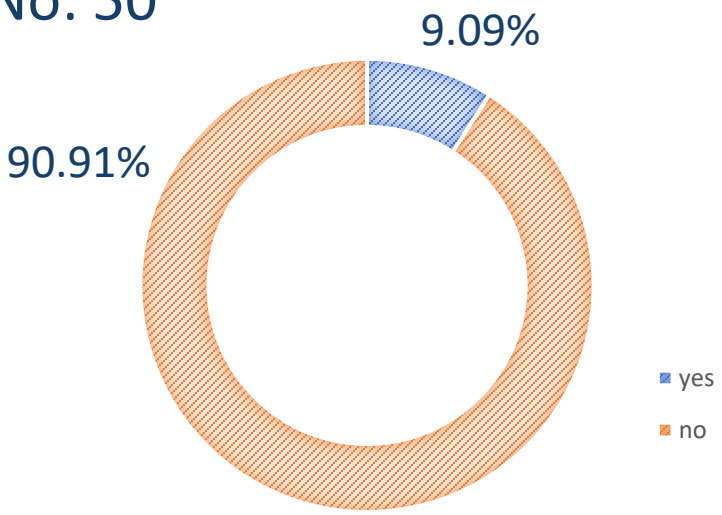
Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)

AUBURN UNIVERSITY
SAMUEL GINN
COLLEGE OF ENGINEERING

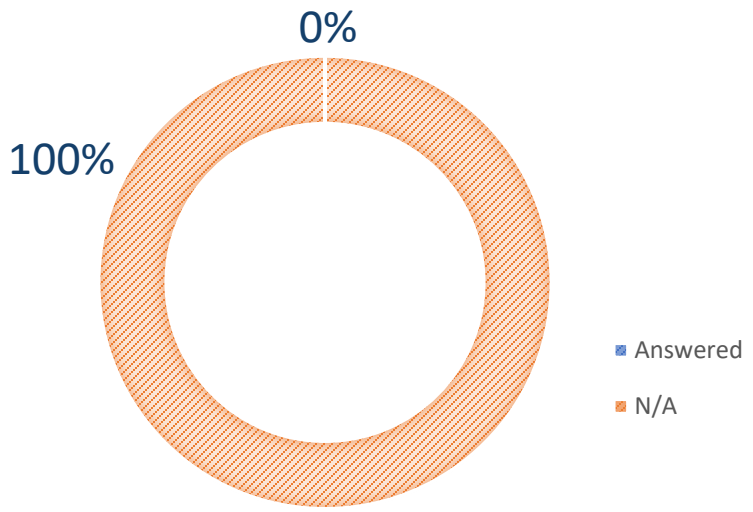
- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

AM Community Survey

- Q20 - Has your organization experienced a cyber incident related to AM activities?
  - Yes: 5
  - No: 50



- Q21 - Please outline your cyber incident experience (if possible).
  - Respondents answered: 0



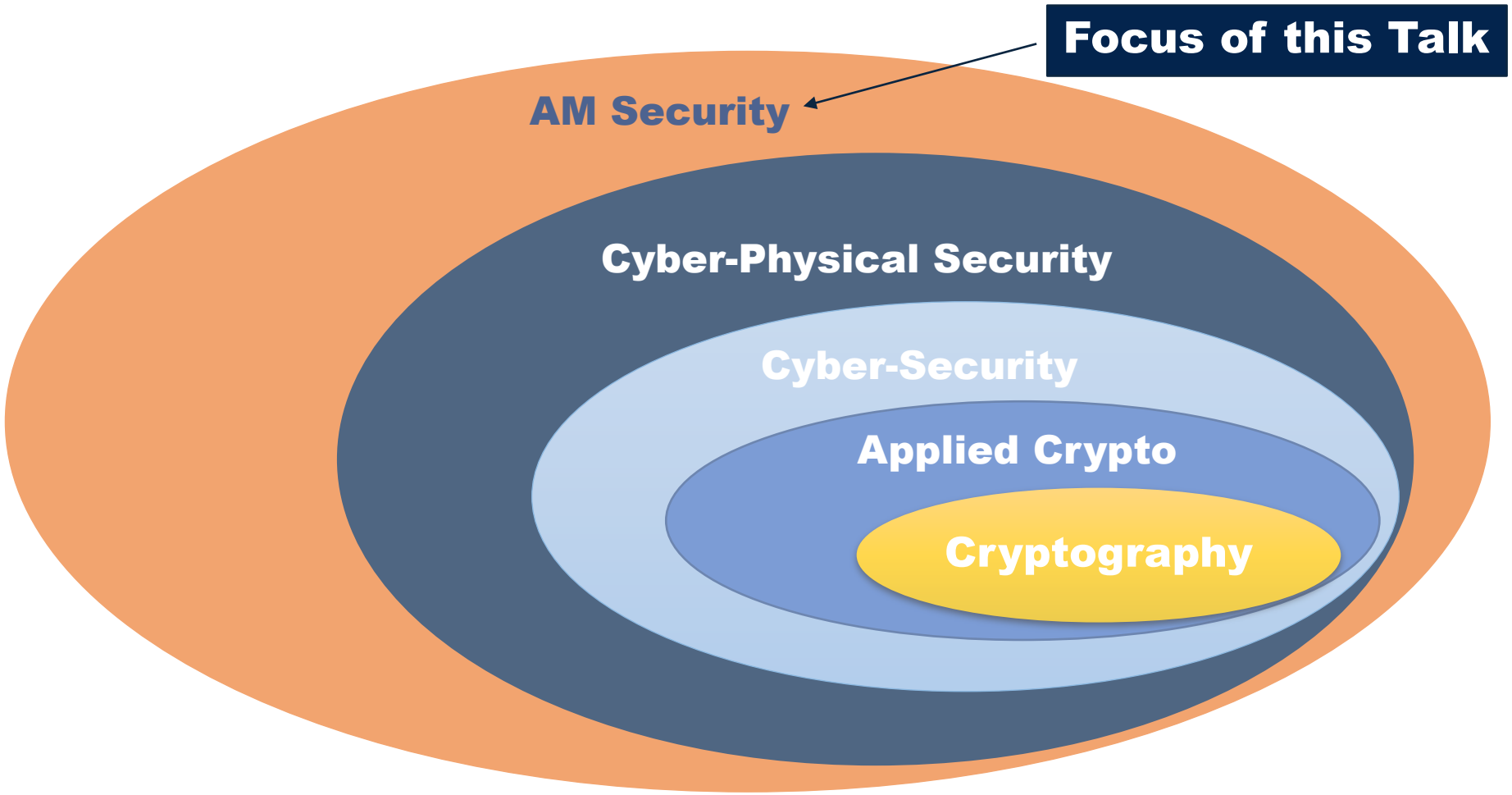
Yampolskiy et al., "State of Security Awareness in the Additive Manufacturing Industry: 2020 Survey." ASTM International Conference on Additive Manufacturing (ICAM 2021), pp. 192-212, 2022.

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

“Zoo” of Security Disciplines

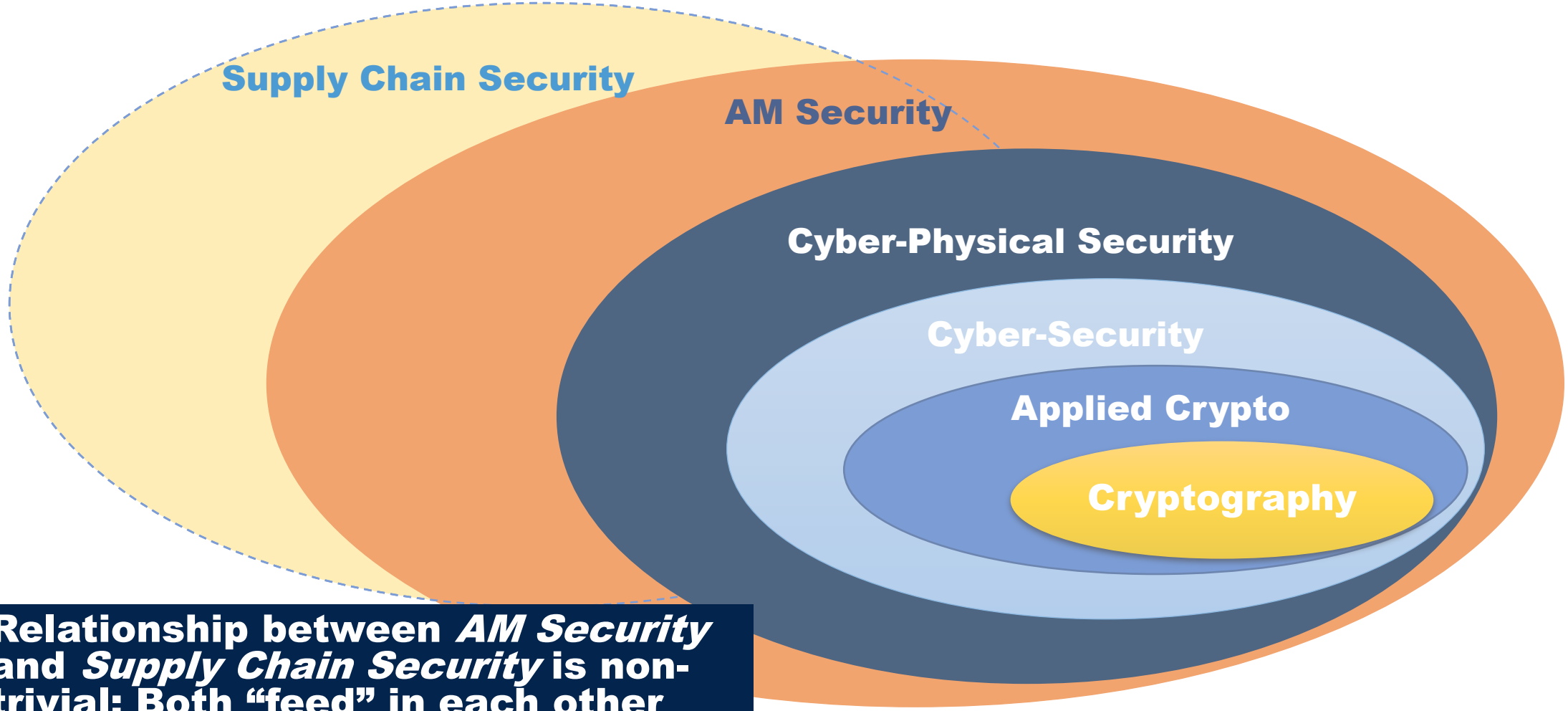
Security Disciplines (1)



Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN
COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

Security Disciplines (2)



Relationship between *AM Security* and *Supply Chain Security* is non-trivial: Both "feed" in each other

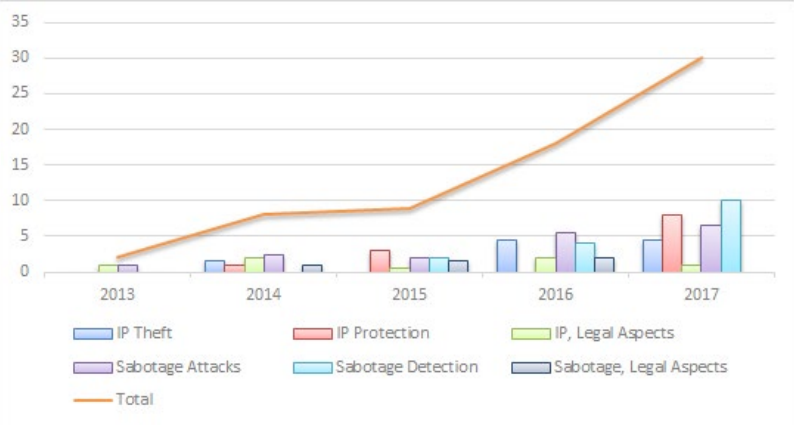
Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN
COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

AM Security Research

How it all Began

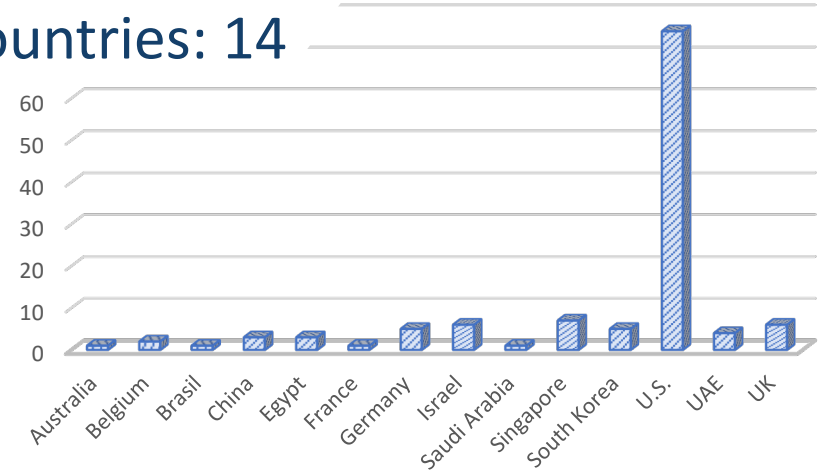
- Pioneered: 2013/2014
- State: End 2017
  - Publications: 67



Yampolskiy et el., "Security of Additive Manufacturing: Attack Taxonomy and Survey." Additive Manufacturing, vol. 21, pp. 431-457, 2018.

More Recent Landscape

- State: April 2019
  - Publications: 113
  - Authors: 214
  - Institutions: 78
  - Countries: 14



Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)

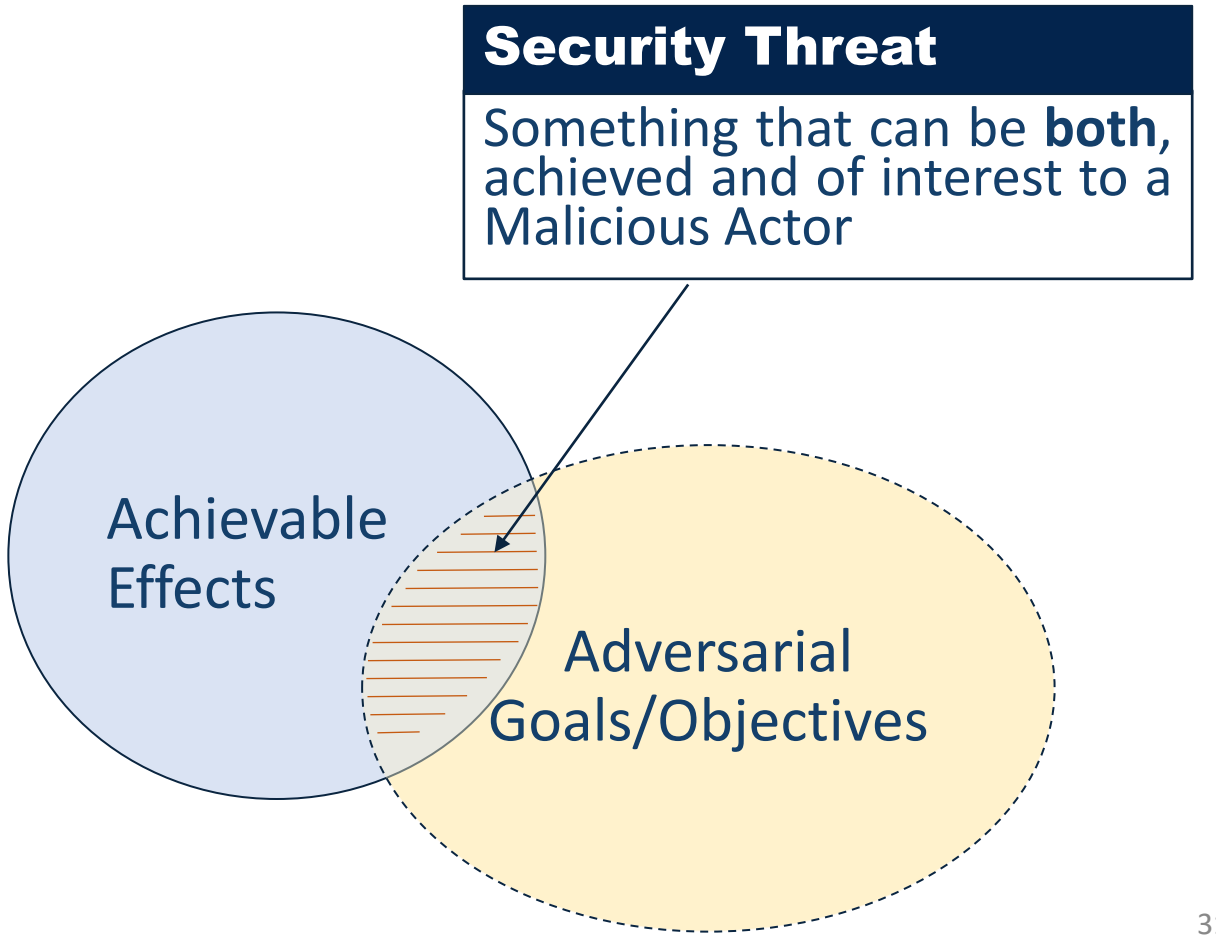
AUBURN UNIVERSITY
SAMUEL GINN
COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

Security Threats in AM

Security Threat Origins

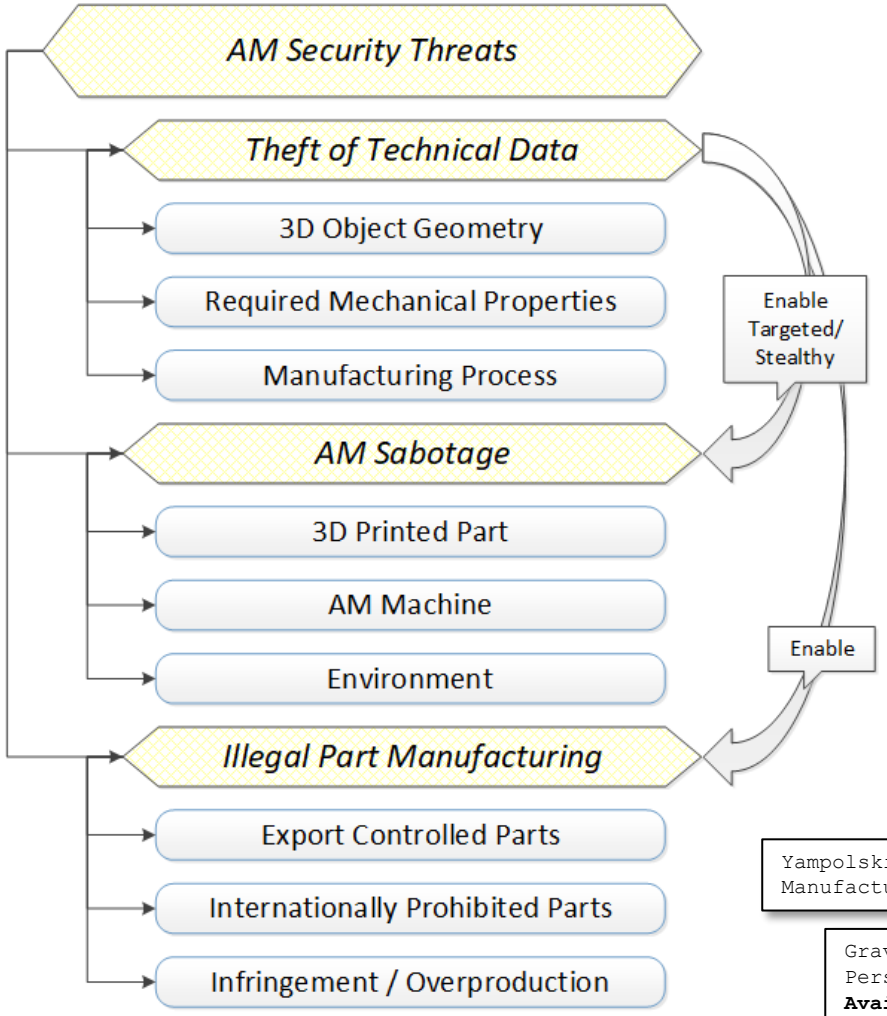
- **Security Threat** – potential malevolent results of an attack (e.g., obtaining, damaging, or destroying an asset of value)
  - = What an adversary **could** do
- **Security Risk** – an applied metric considering use case-specific
  - (i) Likelihood/ probability of Security Threat to realize (=what an adversary **would** do) and
  - (ii) Potential negative impact (loss of revenue, market share, etc.)



Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

AM Security Threats



- Threat describes ***malevolent results*** (not ***attack means***)
- Threat Interdependencies exist
- Each Security Threat can be considered from different Perspectives
  - *Attacks Means*
  - *Defense Measures*
  - *Legal Implications*

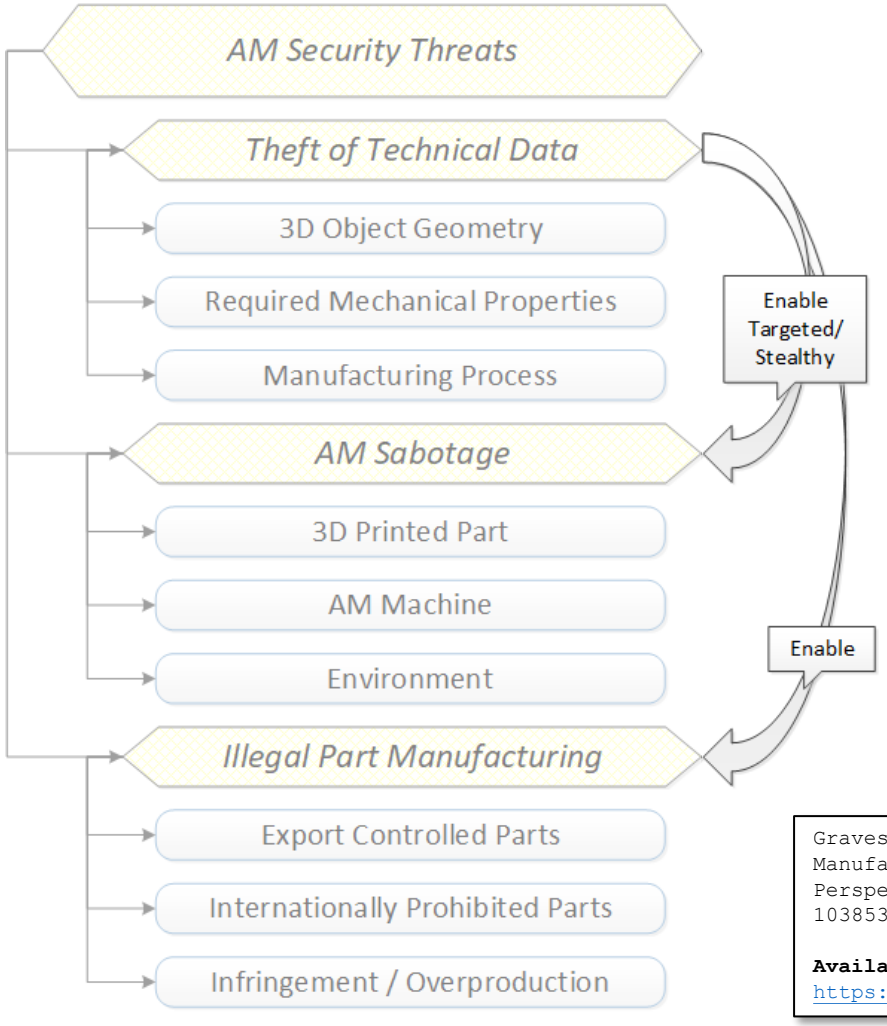
Yampolskiy et al., "Security of Additive Manufacturing: Attack Taxonomy and Survey." Additive Manufacturing, vol. 21, pp. 431-457, 2018.

Graves et al., "Characteristic Aspects of Additive Manufacturing Security From Security Awareness Perspectives." IEEE Access, vol. 7, pp. 103833-103853, 2019.
Available Online (free of charge): https://ieeexplore.ieee.org/abstract/document/8779615`

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

Threat Dependencies



- Technical Data Theft often precedes and enables other threats in AM
  - Enables **targeted** AM Sabotage
    - Specific Part
    - Specific Failure Characteristics
  - Enables Illegal Part Manufacturing
    - Might require protection removal

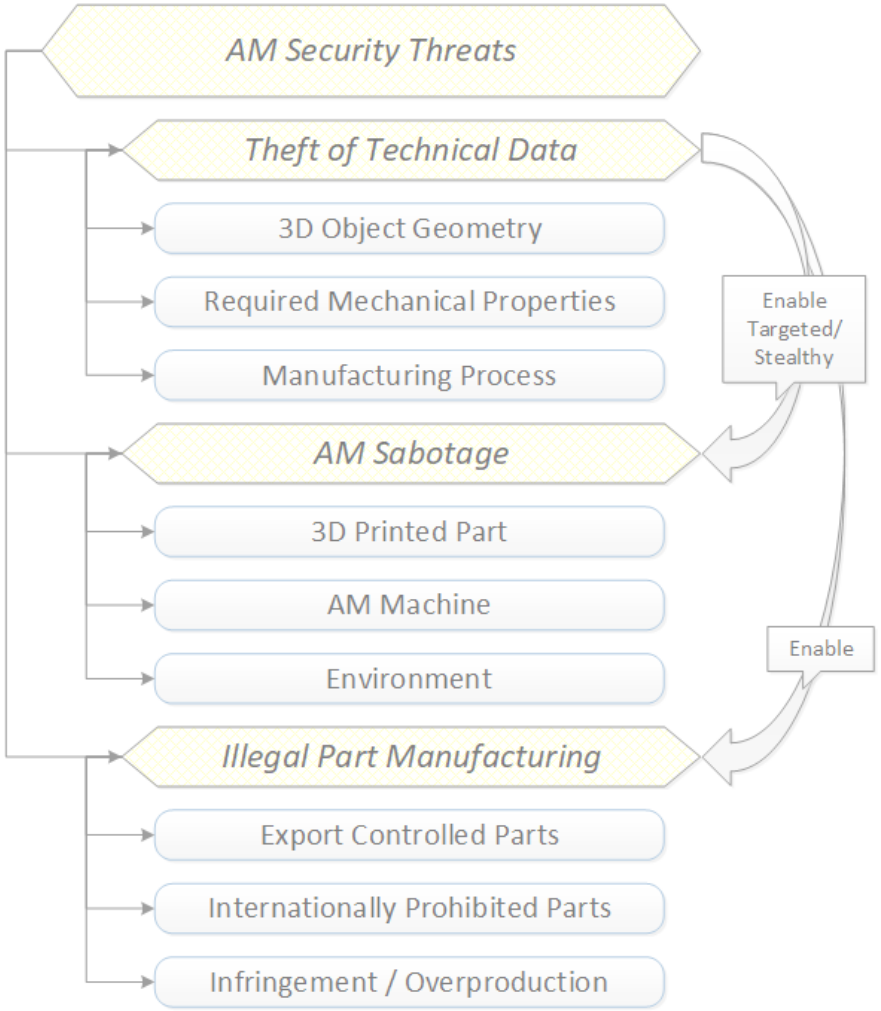
Graves et al., "Characteristic Aspects of Additive Manufacturing Security From Security Awareness Perspectives." IEEE Access, vol. 7, pp. 103833-103853, 2019.

Available Online (free of charge):
https://ieeexplore.ieee.org/abstract/document/8779615

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

Perspectives

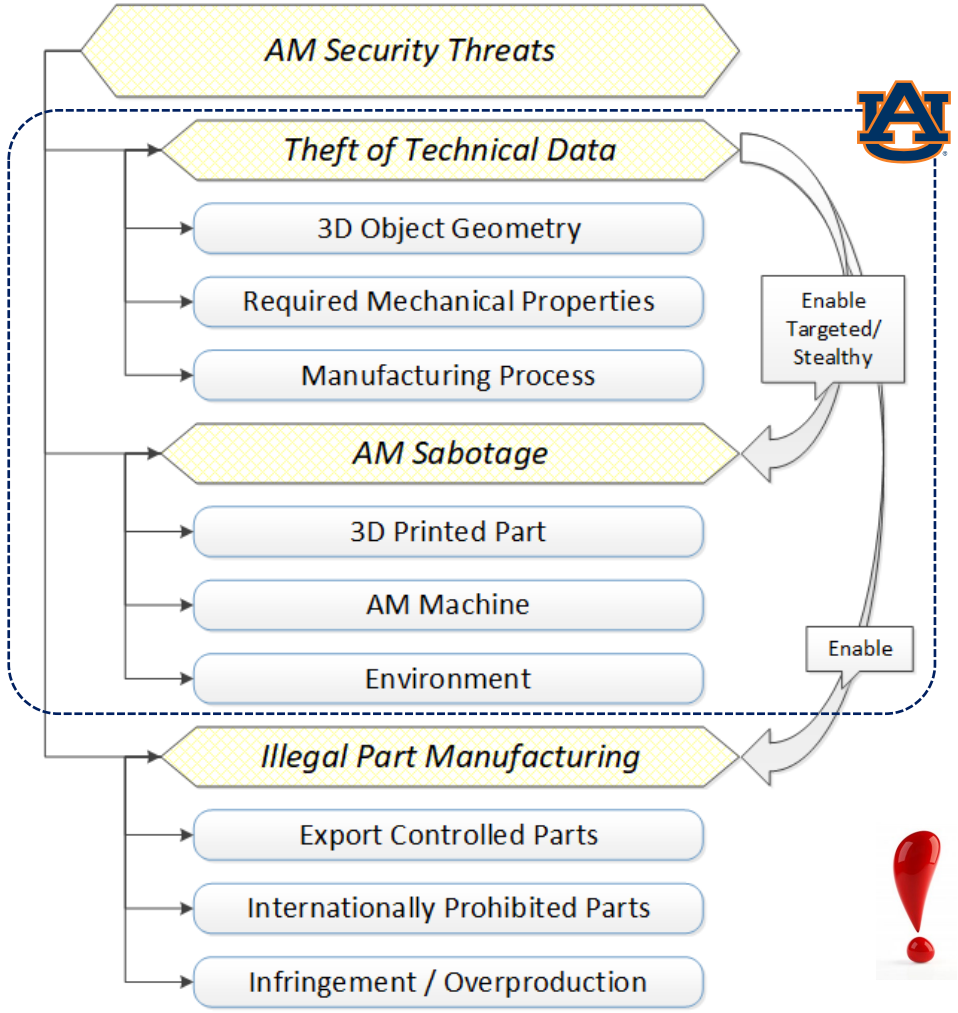


- Each Security Threat can be considered from different Perspectives
  - How attacks can be conducted and by whom
  - How attacks can be prevented or detected
  - What are legal implications in the case of a successful attack

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

AM Security Research @ Auburn University



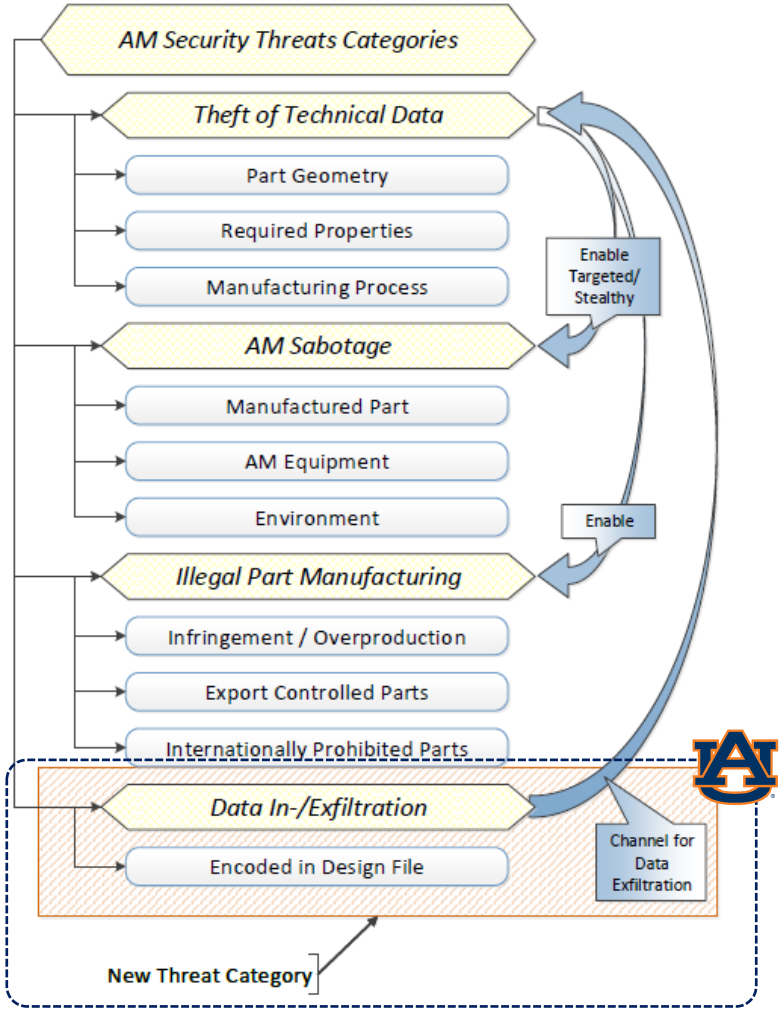
- Threat describes ***malevolent results*** (not ***attack means***)
- Considering Security Threat from different *Perspectives*
  - *Attacks Means*
  - *Defense Measures*
  - *Legal Implications*

Discovered New Security Threat Category – Publication Accepted

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

New Security Threat



- Stego channels exist in …
  - Digital design files (proven for STereoLithography, STL)
  - 3D-printed objects
- Can be used for malicious …
  - Data Infiltration: e.g., Malware into Secure Environment
  - Data Exfiltration: e.g., Stolen sensitive data out of Secure Environment

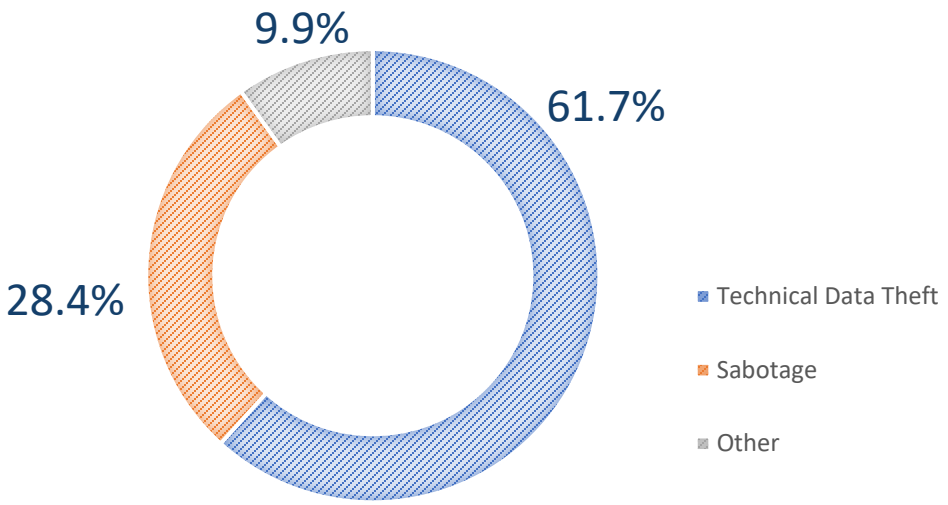
Yampolskiy, M., Graves, L., Gatlin, J., Skjellum, A., Yung, M. "What Did You Add to My Additive Manufacturing Data?: Steganographic Attacks on 3D Printing Files." RAID'21.

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

AM Community Survey

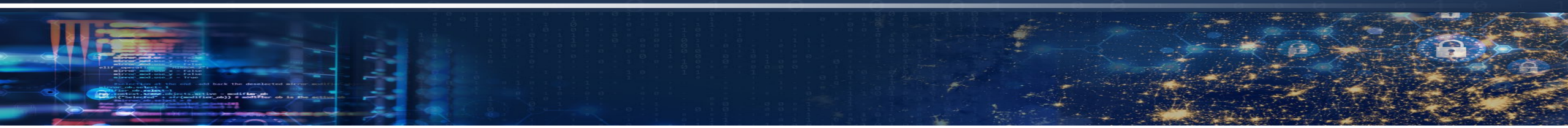
- Q2 - What are your biggest security concerns associated with additive manufacturing (AM)?
  - Technical Data Theft: 50 (61.7%)
  - Sabotage ……: 23 (28.4%)
  - Other ……: 8 (9.9%)
    - *“Violation of export control restrictions”*
    - *“Traceability of material sources”*
    - *“Unintentional data corruption”*
    - *“Liability for tech data theft”*
    - *…*



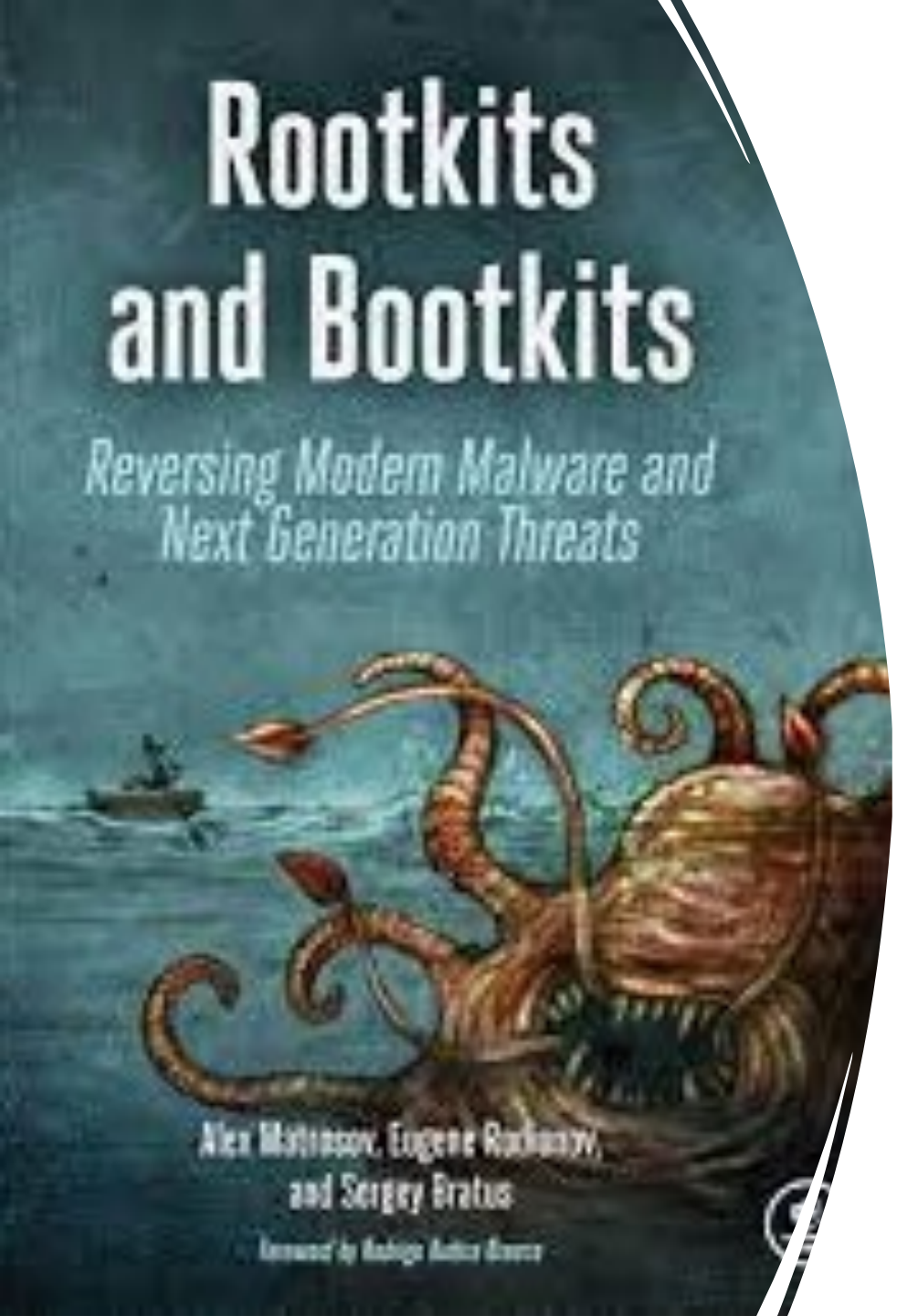
Yampolskiy et al., “State of Security Awareness in the Additive Manufacturing Industry: 2020 Survey.” ASTM International Conference on Additive Manufacturing (ICAM 2021), pp. 192-212, 2022.

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)



Part 2
AM-specific Attacks



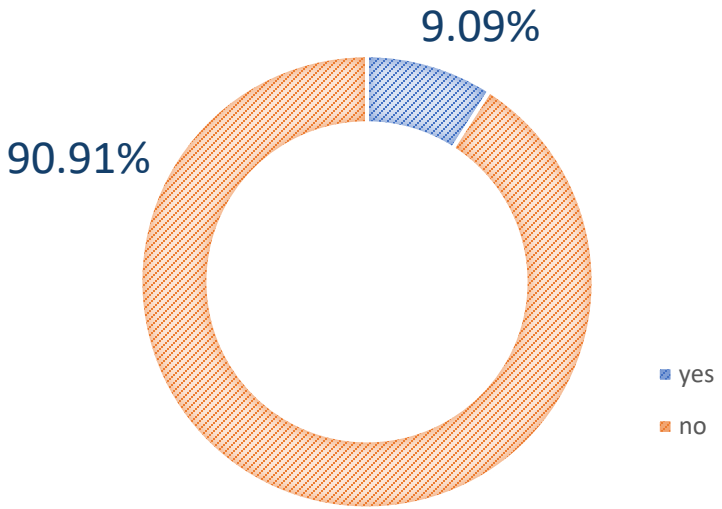
Offense & Defense

"If you shame attack research, you misjudge its contribution. Offense and defense aren't peers. Defense is offense's child."

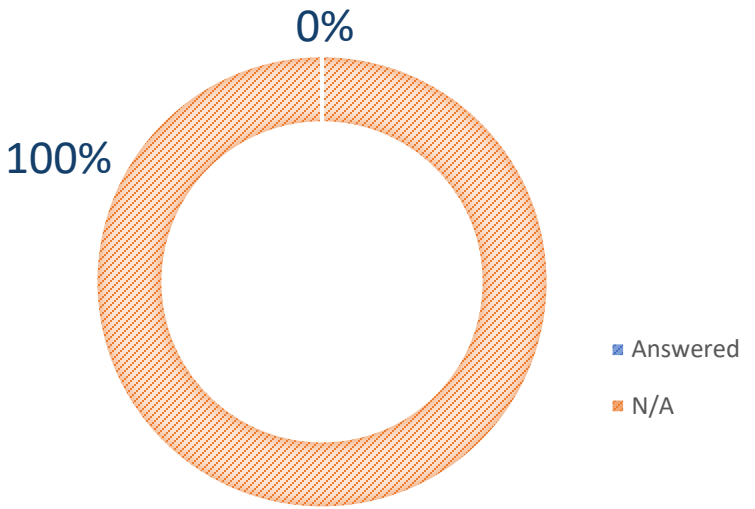
– John Lambert (Microsoft senior security researcher)

AM Community Survey

- Q20 - Has your organization experienced a cyber incident related to AM activities?
  - Yes: 5
  - No: 50



- Q21 - Please outline your cyber incident experience (if possible).
  - Respondents answered: 0

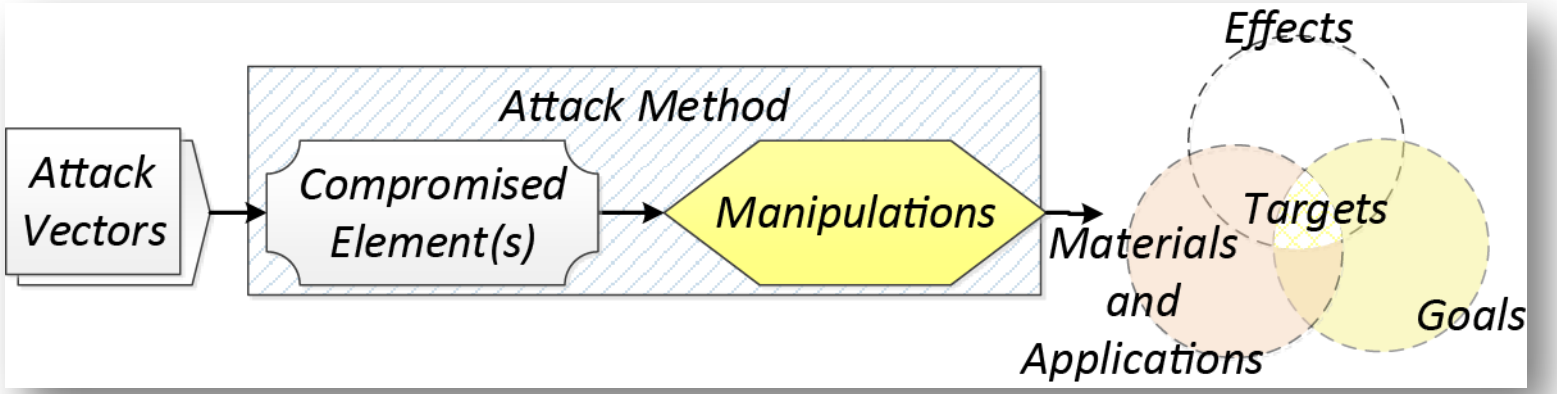


Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN
COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

Attack Analysis

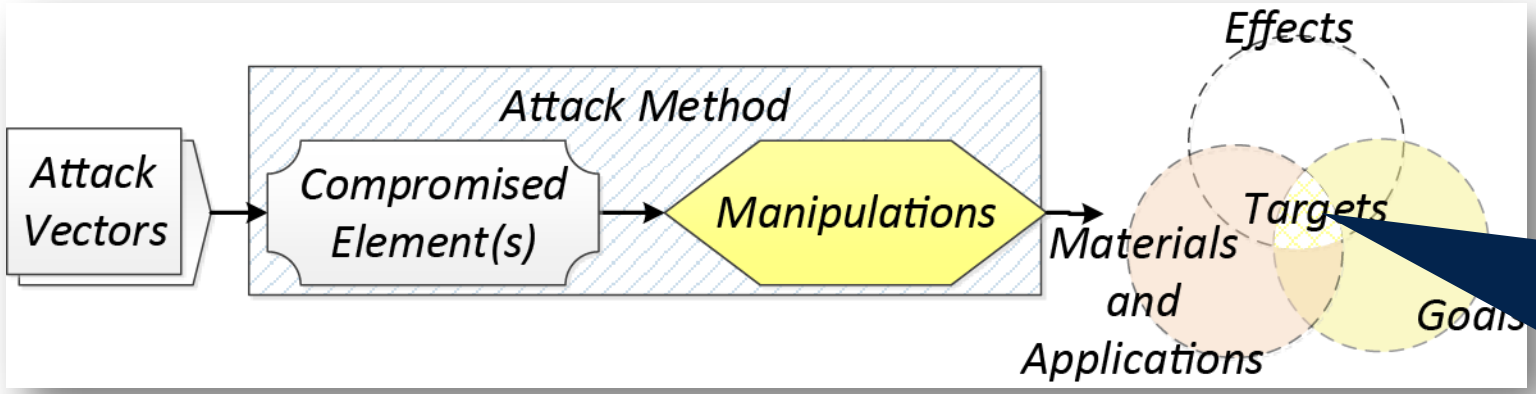
- Attack Analysis Framework
  - Provides a Way for Systematically "Dissect" Attacks on/with AM
  - Helps to Cope with Multi-Domain Complexity of AM Security



Yampolskiy et al., "Using 3D Printers as Weapons." International Journal of Critical Infrastructure Protection, vol. 14, pp. 58-71, 2016.

Yampolskiy et al., "Security of Additive Manufacturing: Attack Taxonomy and Survey." Additive Manufacturing, vol. 21, pp. 431-457, 2018.

Structural Characteristics



What Achievable

Realization of Security Threats depends on factors:

- AM Technology
- Used Materials
- Application Area

How to Compromise a System

- Independent from Security Threat
- Huge Overlap with Cyber-Security

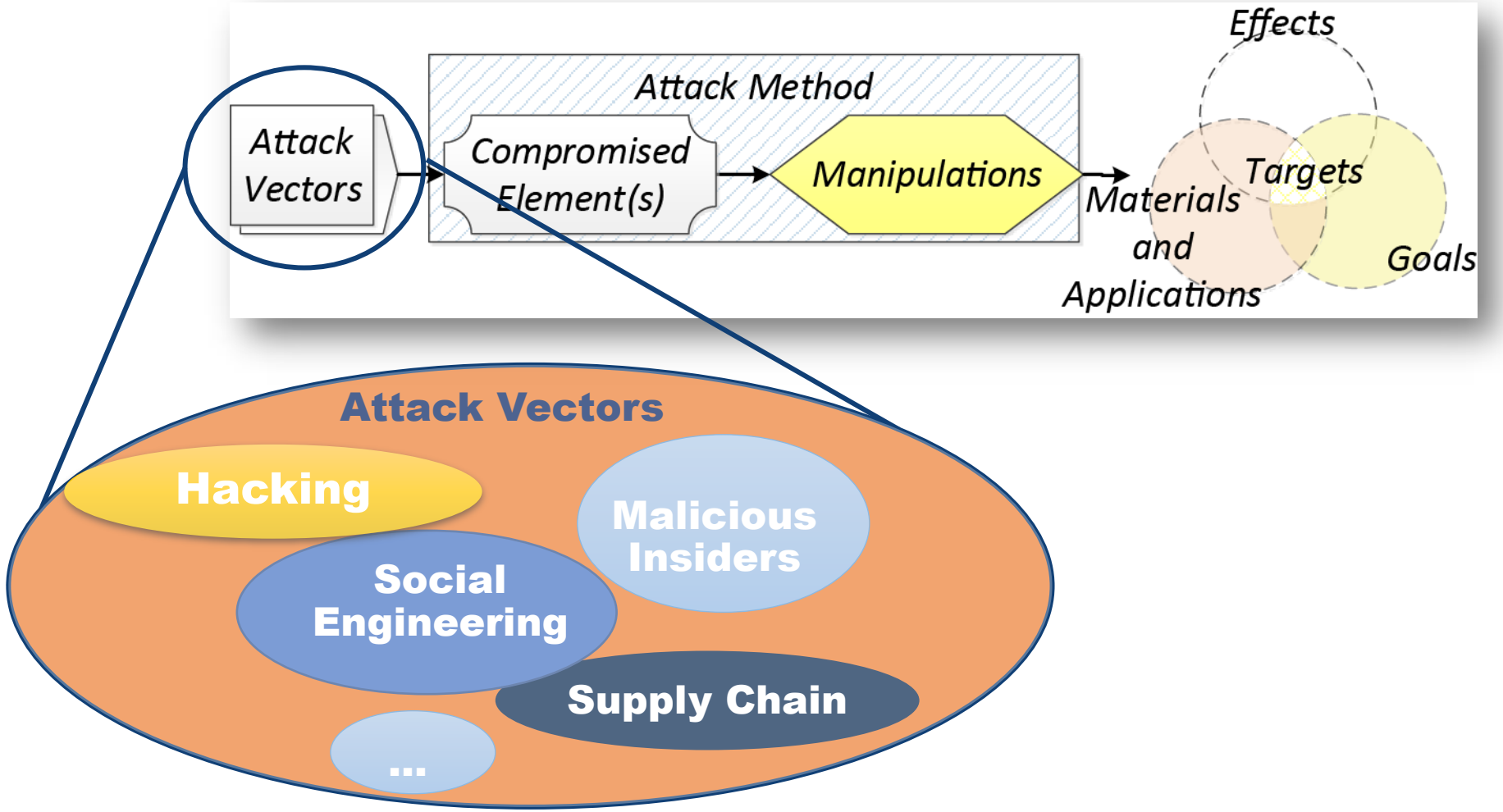
How to Conduct an Attack

- Security Threat Specific
- Attack Methods: Cyber-, Physical, and Cyber-Physical
- AM Process-Dependent

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

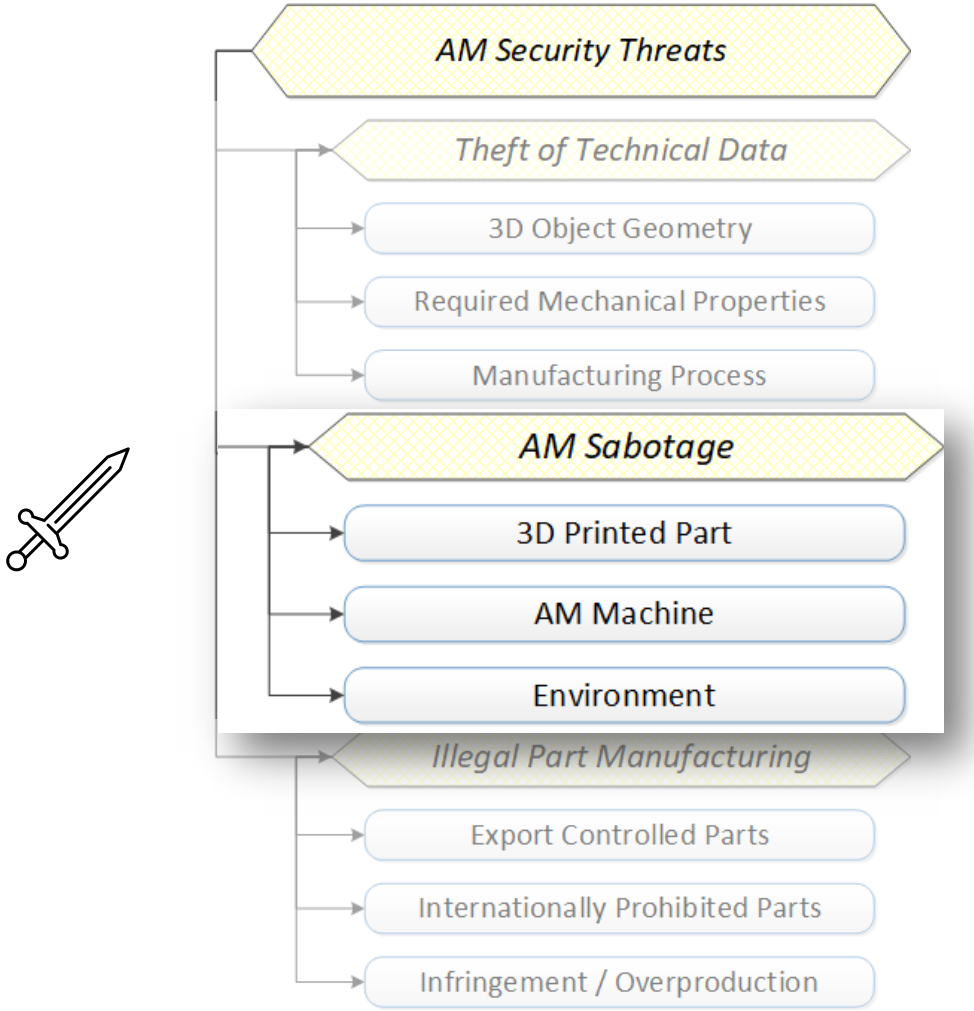
Classical Attacks in AM



Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

AM Sabotage (1)

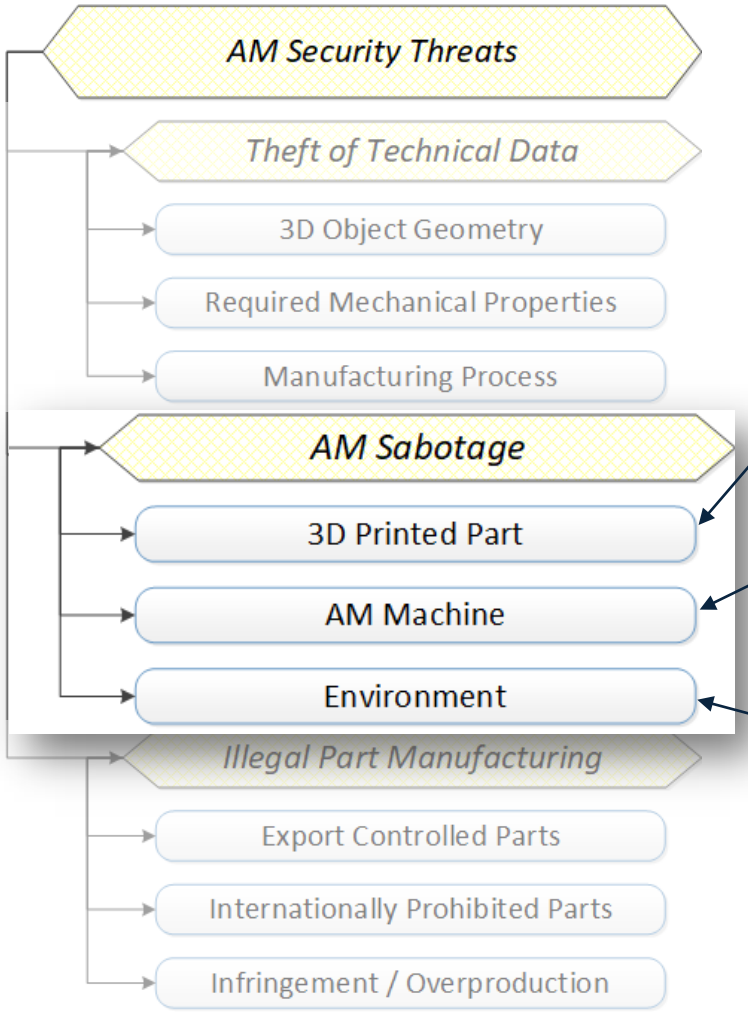


- Sometimes, *"Integrity Violation"* is used to describe, but it does not always lead to a sabotage
  - Designs of functional parts usually have a *safety factor* – degradation within tolerances causes no harm
  - Similarly, AM Machines are built with safety considerations
  - AM Process itself is exposed to a degree of stochastic fluctuations
  - Introduced changes might even improve part's characteristics

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

AM Sabotage (2)

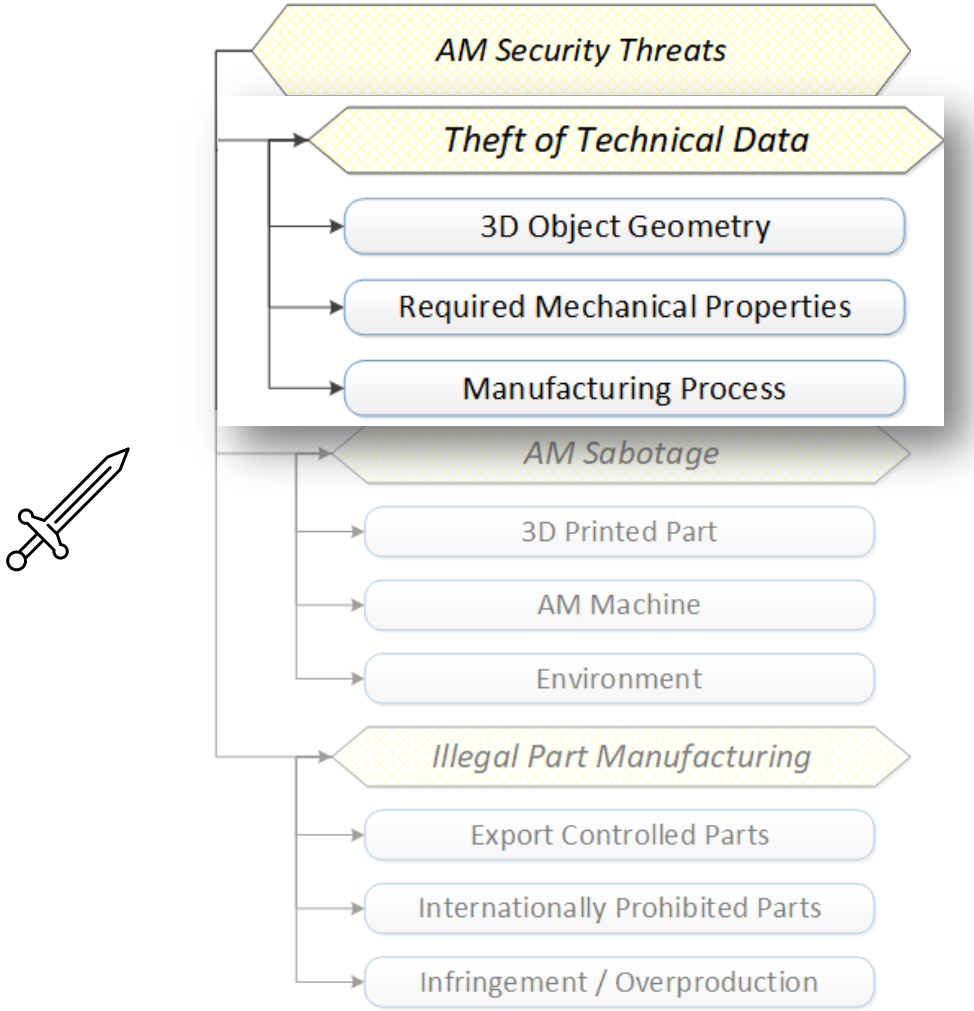


- 3D Printed Part
  - Form, Fit, and Function (FFF) of a 3D-printed part are most obvious sabotage targets
- AM Machine
  - Damage of sub-systems can delay manufacturing, increase costs
- Environment
  - Working with hazardous materials such as flammable or combustible powders enables attacks on environment

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

Technical Data Theft

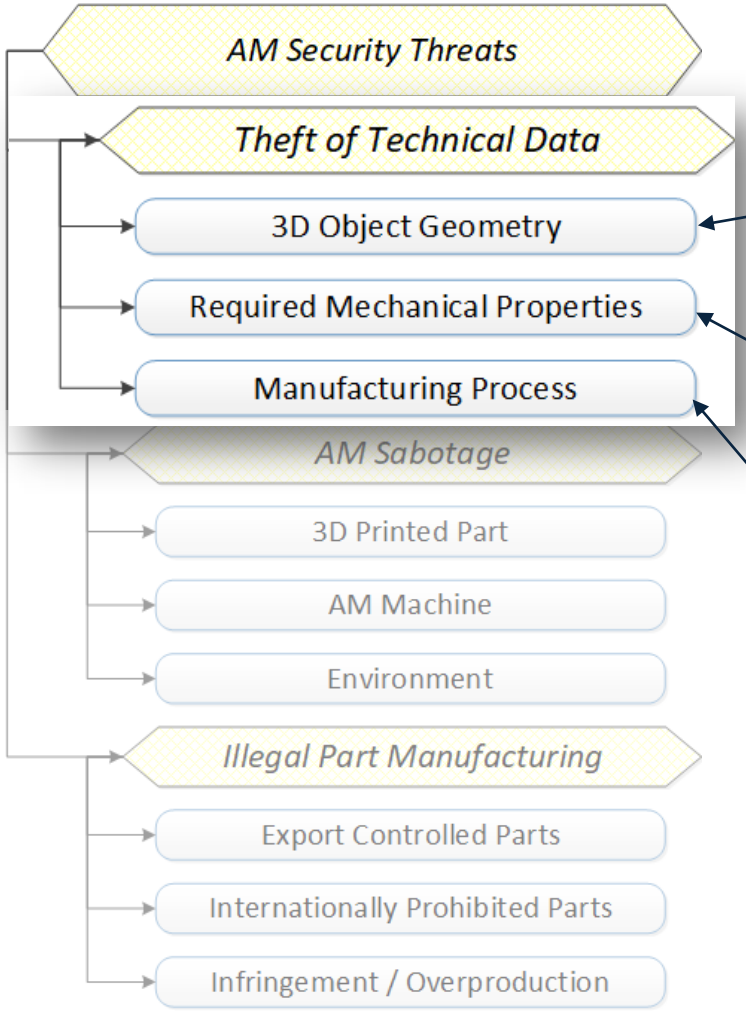


- *"Intellectual Property (IP) Theft"* is often used, but it is not always applicable
  - *Trade Secrets* are not IP
  - Not everything can be protected as IP under current US law
  - Various Technical Data (even if not considered as sensitive) might be used to enable other / follow-up attacks

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

Technical Data Theft (2)



- 3D Object Geometry
  - Digital Design for 3D Printing
  - File Formats: STL, AMF, 3MF, etc.
  - Needed, e.g., for Infringement
- Required Mechanical Properties
  - Provide insights about part's operational conditions
- Manufacturing Process
  - Often seen as a "Secret Sauce" that allows to manufacture parts with required characteristics

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

Malicious AM Service Provider

- *Gatlin et al.*, 2021
  - AM Process: FDM
  - Compromised Element
    - Malicious Manufacturer
  - Attack Method
    - Actuators of 3D Printer instrumented with inductive current probes
    - Measure power supply to actuators
  - Effects
    - Accurate reconstruction of 3D-printed models
- Attack Scenario
  - Fully-encrypted AM
  - Man-at-the-End (MATE) Attack

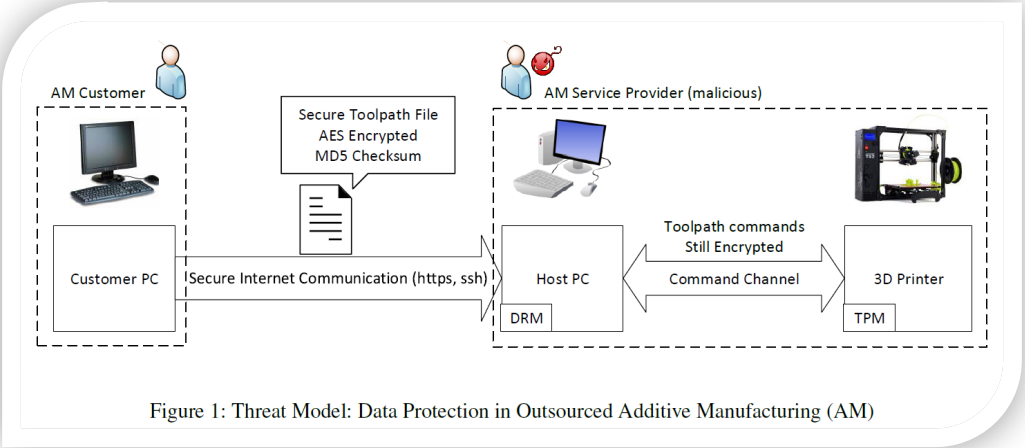


Figure 1: Threat Model: Data Protection in Outsourced Additive Manufacturing (AM)

Gatlin et al., "Encryption is Futile: Bypassing Security for Additive Manufacturing Reconstruction.", 2021 (under review)

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN
COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

Power Side-Channel

Tapping Motor Power

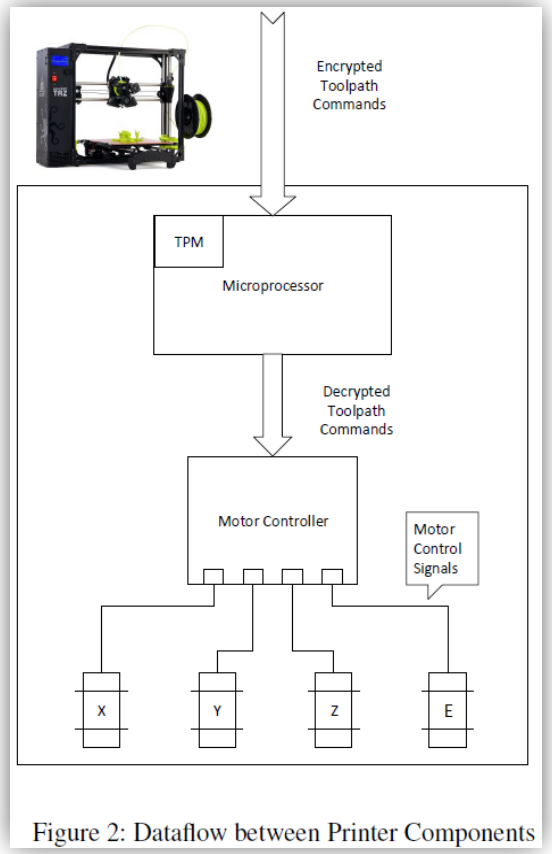


Figure 2: Dataflow between Printer Components

Instrumented 3D Printer

Figure 3: Our Lulzbot Taz 6 printer, instrumented by two Picoscope 5444D oscilloscopes. The probes are 60A Inductive Current Clamp probes, also by Picoscope. Each motor (highlighted) has two clamps attached, one for each phase. The fan controller is also instrumented by a standard voltage probe. The data captured here is transmitted to a host PC running the PicoScope application.

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN
COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

Reconstruction Results

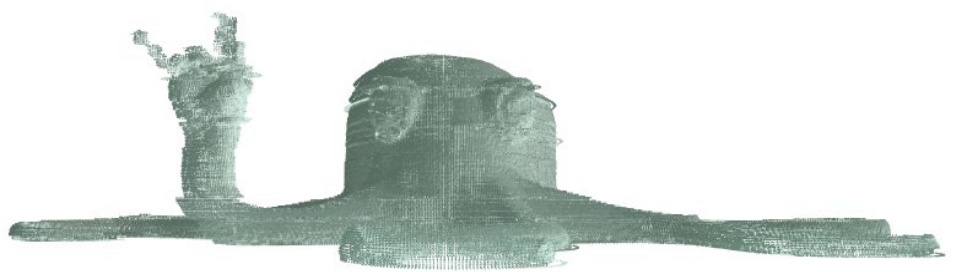
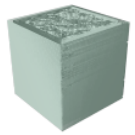
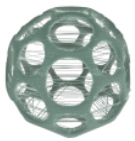
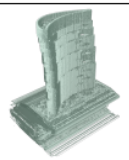
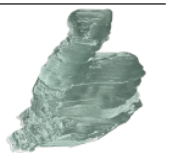


Figure 17: The reconstructed Octopus model, visualized as a point cloud. While the degree of drift present here would not affect the main body of the print, it would likely cause print failure in the fine detail of the raised hand.

In Outsourced AM, Encryption is Futile

Table 2: Point cloud renderings and metrics of the reconstructed models. Any support structure is included in the rendering; the skirt has been removed manually to provide a larger visualization.

Metrics		Render	Metrics		Render
Name:	Cube		Name:	Ninja Star	
Print Duration:	13.63 min		Print Duration:	4.48 min	
Steps Traveled:	98,098		Steps Traveled:	65,534	
Points in Cloud:	80,196		Points in Cloud:	49,297	
Sections:	2,344		Sections:	1,384	
Bad Sections:	351		Bad Sections:	349	
B.S. Max. Length:	2		B.S. Max. Length:	4	
B.S. Avg. Length:	1.00		B.S. Avg. Length:	1.1	
Name:	Wrench		Name:	Rook	
Print Duration:	44.33 min		Print Duration:	49.98 min	
Steps Traveled:	774,063		Steps Traveled:	429,117	
Points in Cloud:	563,305		Points in Cloud:	340,909	
Sections:	21,445		Sections:	23,735	
Bad Sections:	5,334		Bad Sections:	6,497	
B.S. Max. Length:	7		B.S. Max. Length:	9	
B.S. Avg. Length:	1.05		B.S. Avg. Length:	1.15	
Name:	Gear		Name:	Bucky Ball	
Print Duration:	50 min		Print Duration:	154 min	
Steps Traveled:	728,078		Steps Traveled:	1,731,428	
Points in Cloud:	611,807		Points in Cloud:	1,126,327	
Sections:	25,893		Sections:	68,796	
Bad Sections:	5,572		Bad Sections:	21,269	
B.S. Max. Length:	6		B.S. Max. Length:	7	
B.S. Avg. Length:	1.15		B.S. Avg. Length:	1.09	
Name:	Octopus		Name:	Turbine Blade	
Print Duration:	66.58 min		Print Duration:	84.98 min	
Steps Traveled:	959,332		Steps Traveled:	879,667	
Points in Cloud:	715,662		Points in Cloud:	629,200	
Sections:	19,375		Sections:	25,192	
Bad Sections:	5,684		Bad Sections:	8,386	
B.S. Max. Length:	7		B.S. Max. Length:	5	
B.S. Avg. Length:	1.08		B.S. Avg. Length:	1.07	
Name:	Stan. Bunny		Name:	Stan. Lucy	
Print Duration:	302 min		Print Duration:	242 min	
Steps Traveled:	5,629,158		Steps Traveled:	3,827,019	
Points in Cloud:	4,490,563		Points in Cloud:	2,578,250	
Sections:	82,030		Sections:	98,730	
Bad Sections:	23,167		Bad Sections:	29,193	
B.S. Max. Length:	11		B.S. Max. Length:	7	
B.S. Avg. Length:	1.10		B.S. Avg. Length:	1.13	

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)

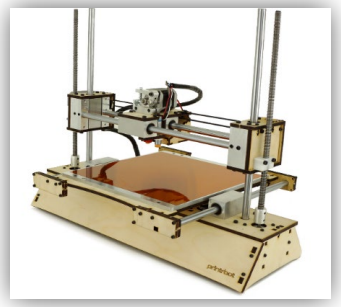
AUBURN UNIVERSITY
SAMUEL GINN
COLLEGE OF ENGINEERING

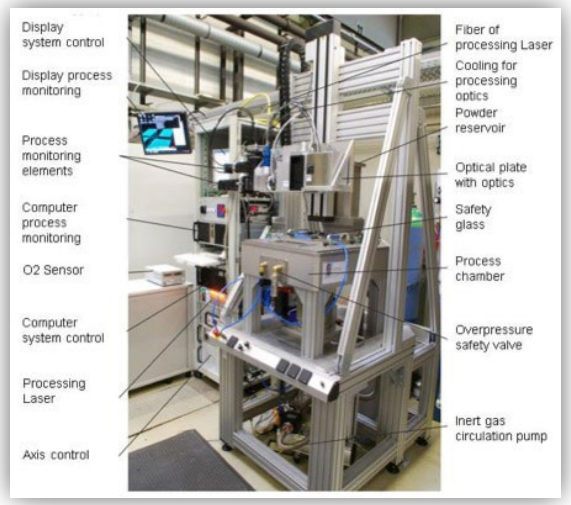
- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

Intermediate Conclusion

Current & Needed – Attacks

	Current	Needed
3D Printers	Desktop	Industrial-Grade
AM Processes	FDM	PBF, DED
Materials	Polymers	Metals, Composites
Attacks	Attack Categories	Optimal / Stealthy





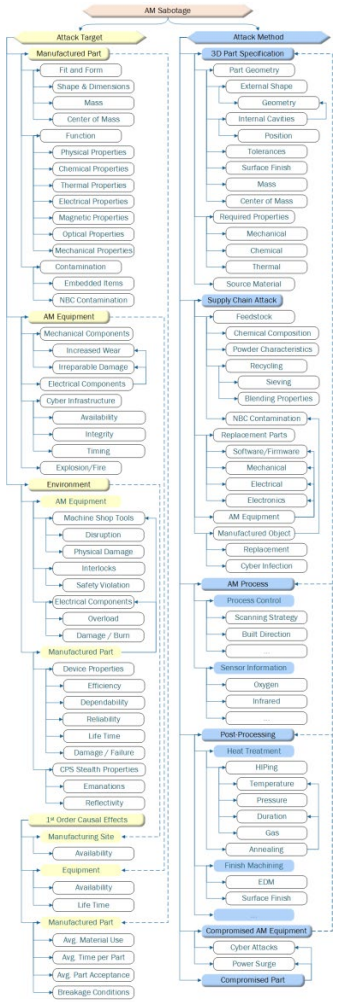
It is important to study attacks to:
- **Identify needed defenses measures**
- **Evaluate defense measures effectiveness**

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING

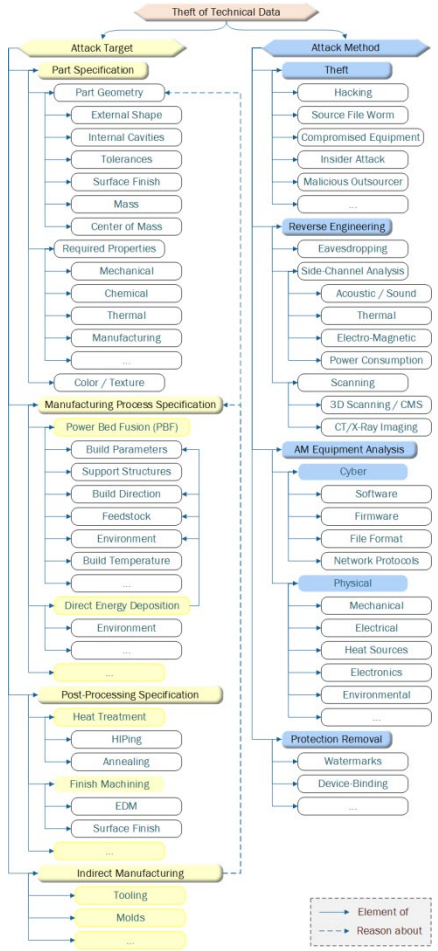
- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

Attack Taxonomies

Sabotage Attacks



Theft of Technical Data



- Taxonomy Dimensions
  - Attack Targets (Security Threats)
  - Attack Methods
- Targets & Methods Correlation

Only few Taxonomy Elements have been Addressed in AM Security Literature (so far)

Yampolskiy et al., "Security of Additive Manufacturing: Attack Taxonomy and Survey." Additive Manufacturing, vol. 21, pp. 431-457, 2018.

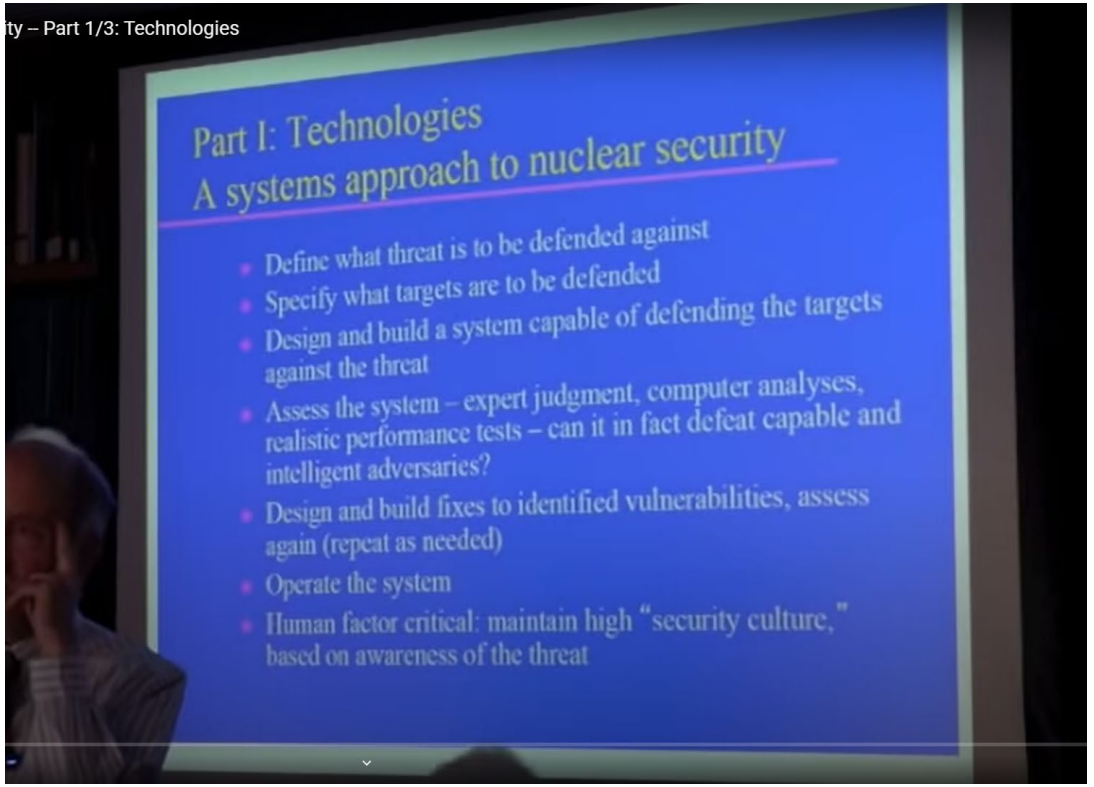
Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

Few Lessons Learned from Nuclear Security

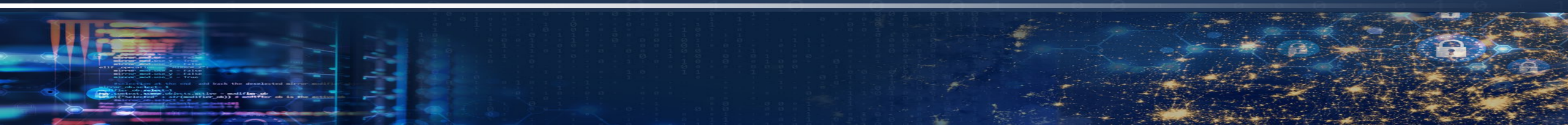
- "There are a lot of things that actually look great on paper or in a computer analysis, that collapse like a house of cards in a face of a really intelligent person thinking *'hmm… oh, I've got an idea how to overcome that'* "
- "The bad guys will do what you have not thought of – that's the problem"

– Matthew Bunn



Matthew Bunn, "Nuclear 101: Technology and Institutions for Nuclear Security -- Part 1/3: Technologies", Belfer Center, 2013

Online on YouTube: https://www.youtube.com/watch?v=2bw1xoO1DAk&list=TLPQMDkwMTIwMjHyR5QjVHFCUQ&index=18



Part 3
AM-specific Defenses

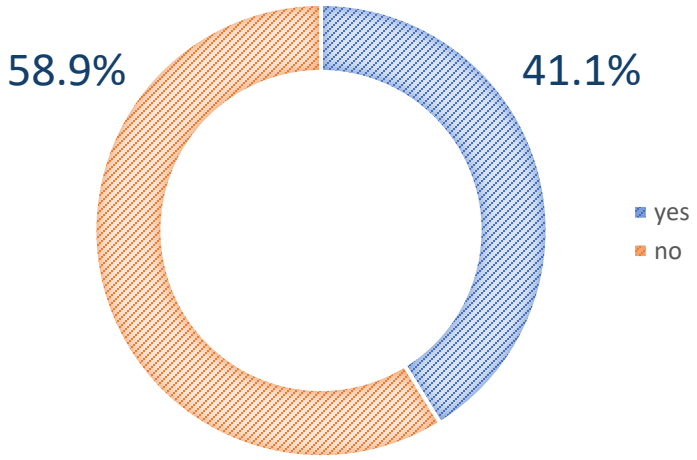
Lessons from Cyber-Security

- "… it is not about ``*show me a smoking gun*'' – this is about ``*adversary has a loaded gun.*'' Why would you stand in front of it?"
- – *Rob Joyce (NSA's Director of Cybersecurity)*

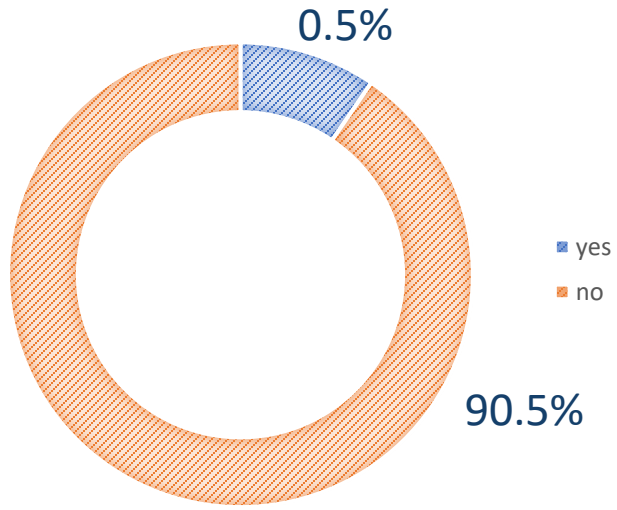
A Conversation on Cybersecurity with NSA's Rob Joyce, Apr 11, 2023
YouTube: https://www.youtube.com/watch?v=MMNHNjKp4Gs&list=TLPQMTUwNDIwMjPmZdOwDeP0SA&index=16

AM Community Survey

- Q #16: Does your organization have a security program for AM?
  - Yes: 21
  - No: 30



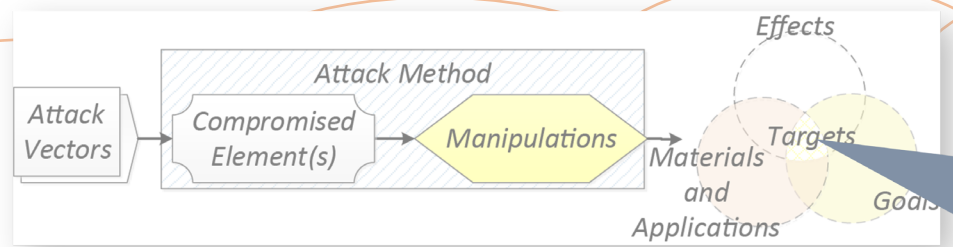
- Q #17: Does it fall under the general cyber-security?
  - Yes: 19
  - No: 2



Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN
COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

Defense Measures



What Achievable

Realization of Security Threats depends on factors:
- AM Technology
- Used Materials
- Application Area

How to Compromise a System
- Independent from Security Threat
- Huge Overlap with Cyber-Security

How to Conduct an Attack
- Security Threat Specific
- Attack Methods: Cyber-, Physical, and Cyber-Physical
- AM Process-Dependent

Before Attack
- System Hardening
- Integration of protection measures

During Attack
- Attack Prevention
- Attack Detection
- Impact minimization

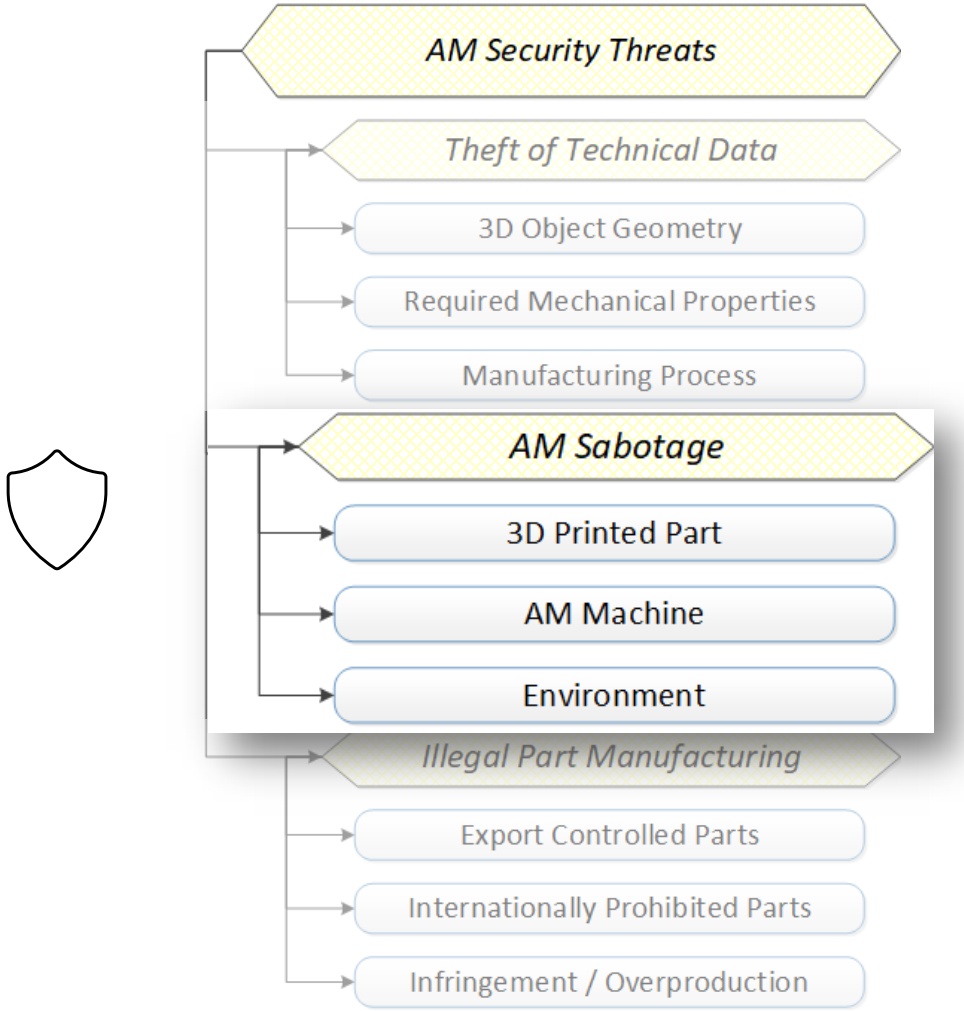
After Attack
- Detection/ Identification
- Attack Investigation/ Forensics
- Attack Attribution

Vary for different Security Threats

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

AM Sabotage Detection



- Sabotage Detection (in the AM context) – identification that the part is produced not in accordance to the specification
  - Regardless of modification and
  - Regardless where introduced
- Side-channel-based Detection – relies on one or multiple side-channels of 3D printer

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN
COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

AM Sabotage Detection (1)

Signature Generation

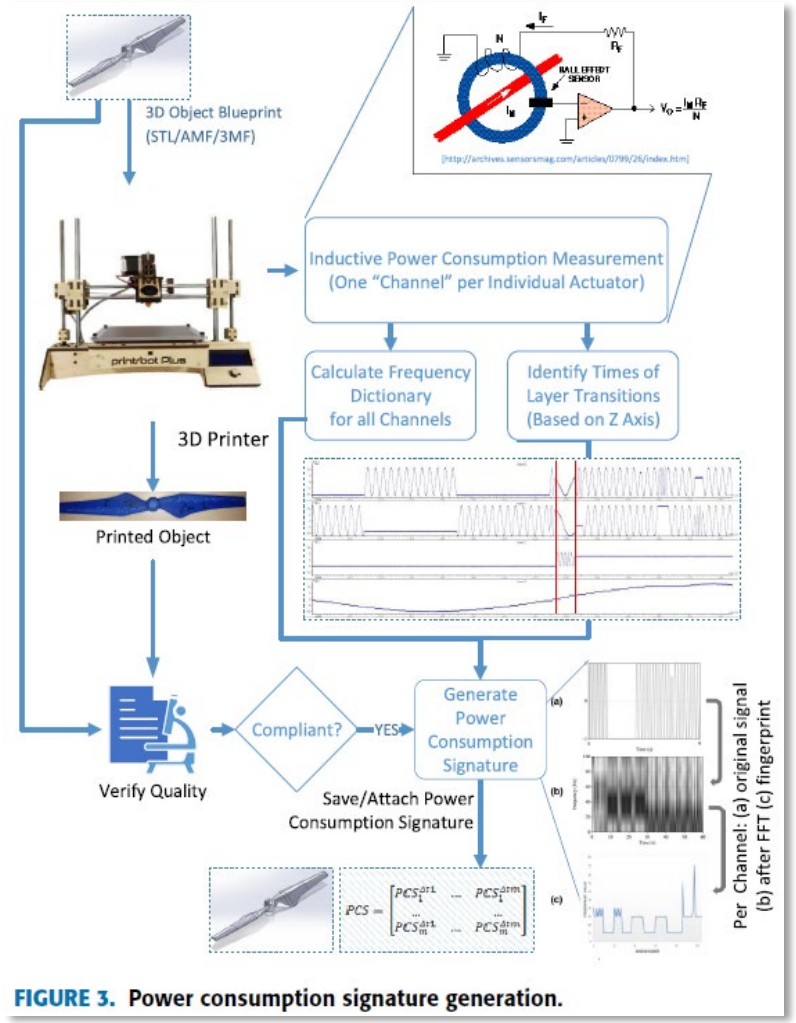


FIGURE 3. Power consumption signature generation.

Signature Comparison

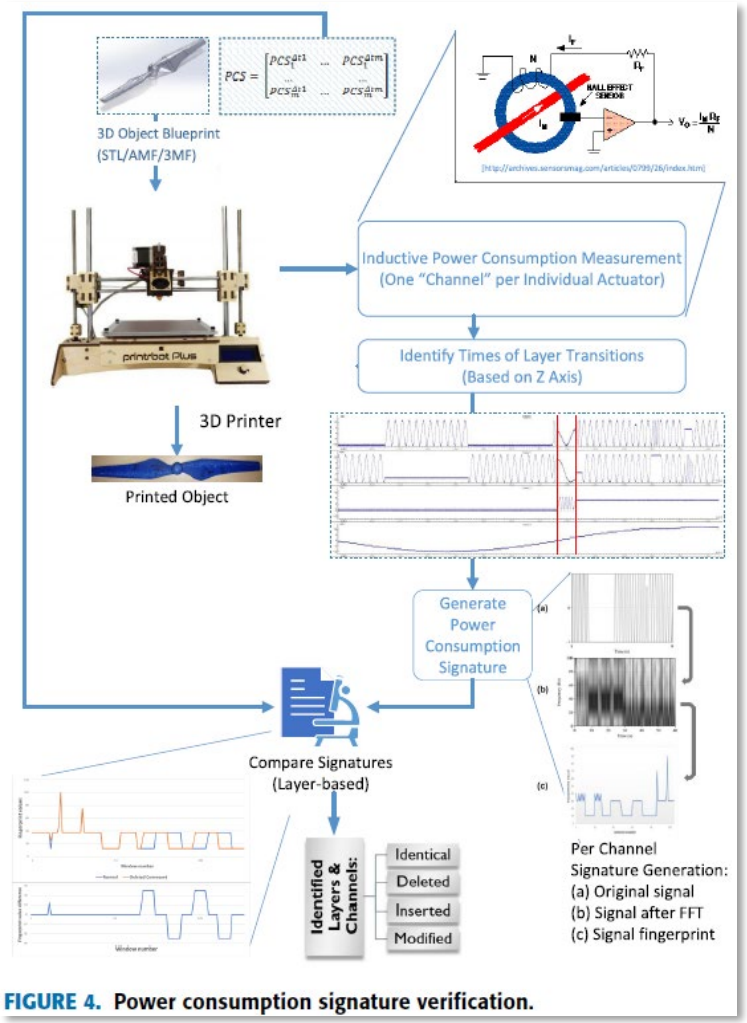


FIGURE 4. Power consumption signature verification.

Gatlin et al., "Detecting sabotage attacks in additive manufacturing using actuator power signatures." IEEE Access, vol. 7, pp. 133421-133432, 2019.

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

AM Sabotage Detection (2)

Characteristics

- Signature
  - Individual channels: PCA-based, like in *Belikovetsky et al.*, 2018
  - Signature is a *channel-layer* matrix
    - Allows "narrowing down" to layer and motor (x/y/z/e) signals that have been altered
- Quality Assessment
  - Detectability of a single G-Code command modification
  - Detectability of known attacks

Detectable Attacks

Level of Modification Detectability		
Modification	**Entire Print**	**Single Layer**
Insertion of Commands	✓	✓
Deletion of Commands	✓	✓
Command Reordering	✓	✓
Layer transition duration	✓	X
"Smart Voids"	X	X

SABOTAGE ATTACK	PROPOSED BY	DETECTED?
Gap/Void	[2, 19]	✓
Contaminant Material	[28]	*N/A*
Different layer thickness	[21]	✓
Scale of the Printed Object	[23]	✓
Amount of Extruded Filament	[15]	*x*
Z-Orientation	[26, 28]	✓
Orientation in *X*-*Y* Plane	[28]	✓
Temperature of Extruded Filament	[23]	*x*

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING

Advantages & Drawbacks

Approach Advantages 

- Non-invasiveness in AM process that is **often Real Time Critical**
- Independence of SW/FW
- Can be retrofitted on already deployed AM equipment
- Can be Air-Gapped
  - Increases difficulty of simultaneous compromise of both monitoring & monitored systems

Approach Limitations 

- Different Side-Channels
  - Are actuator-dependent
    - Limited to certain AM Process only
  - Require different type and degree of 3D Printer instrumentation
    - Might violate OEM's EULA
- All approaches are limited by detectability thresholds
  - Attacks might remain undetected

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING
• Auburn Cyber Research Center (ACRC)
• National Center for Additive Manufacturing Excellence (NCAME)

Intermediate Conclusion

Defense Measures

	Current	Needed
3D Printers	Desktop	Industrial-Grade
AM Processes	FDM	PBF, DED
Materials	Polymers	Metals, Composites
Defense Measures	Proof of Concept for Chosen Attacks	• Thresholds (e.g., for Detectability) • Robustness against Countermeasures
Assessment	Authors' Custom-Made	***Standards*** to measure/assess/compare

Same as Attacks

No real attacker will try to make it easy for defender

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)

AUBURN UNIVERSITY
SAMUEL GINN
COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

Defense Measures

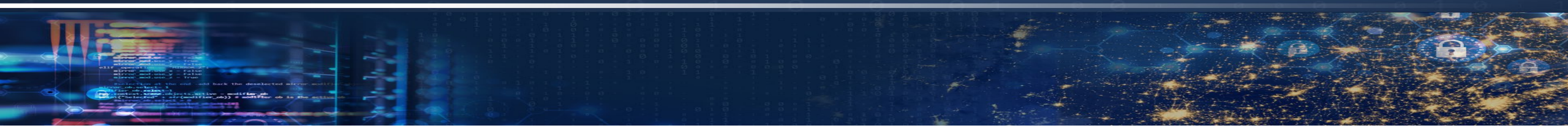
	Current	Needed
FORENSICS	Action Reconstruction	Action Attribution
RESIDUAL DATA	Selected 3D Printer(s)	• Supply Chain • Data Correlation
ANTI-FORENSICS	–	• Delete/Plant Evidence • Detect Anti-Forensics Efforts

Without Analysis of successful attacks, we have no chance to improve and prevail…

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)

AUBURN UNIVERSITY
SAMUEL GINN
COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)



Part 4
Myths and Misconceptions

“Nothing is more dangerous for a new truth than an old misconception.”

— Johann Wolfgang von Goethe

Cybersecurity

Misconception

- Cybersecurity solutions, if applied properly, are fully sufficient to secure AM
- Discussed in AM Community
  - Protect “Data at Rest”
  - Protect “Data in Transit”

Reality in AM

- Cybersecurity solutions are **necessary** component to
  - Protect Digital Data (e.g., Design)
  - Harden SW against compromise
  - Detect/investigate cyber-attacks
- Cybersecurity solutions alone are **not sufficient** to secure AM
  - Limited areas of application in AM
  - Not sufficient to defend against all kinds of attacks in AM

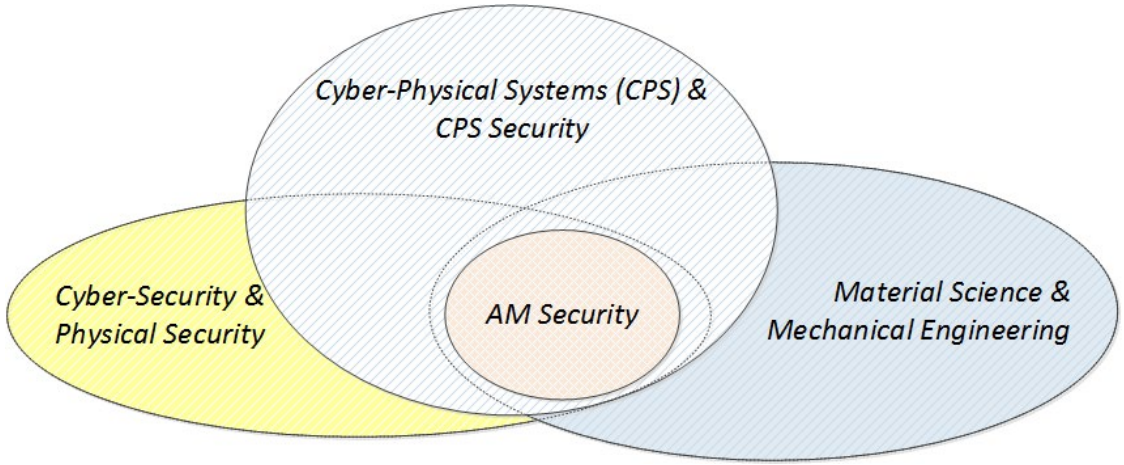
Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

Domain Expertise

Misconception

- Single-domain expertise is sufficient to understand and address all Security issued



Reality in AM

- Single-domain expertise is only sufficient to address few selected security issues
- Multi-Disciplinary Teams needed to understand and address hard problems of AM Security
  - Challenge: Experts from different domains need to collaborate and to understand each other
    - Perspectives/Terminology differ!!

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

Air-Gap

Misconception

- Air-Gap solution work and sufficient to protect against compromise
  - Disconnecting AM from Network and only use USB

Reality in AM

- One of AM big "selling points" is ease of outsourcing
  - Air-Gap will lead to indirect pathways (can be compromised)

"As a theory, the air gap is wonderful. **In real life, it just does not work.** […] As much as we want to pretend otherwise […] Severing the network connection with an air gap simply spawns new pathways like the mobile laptop and the USB flash drive, which are more difficult to manage and just as easy to infect."

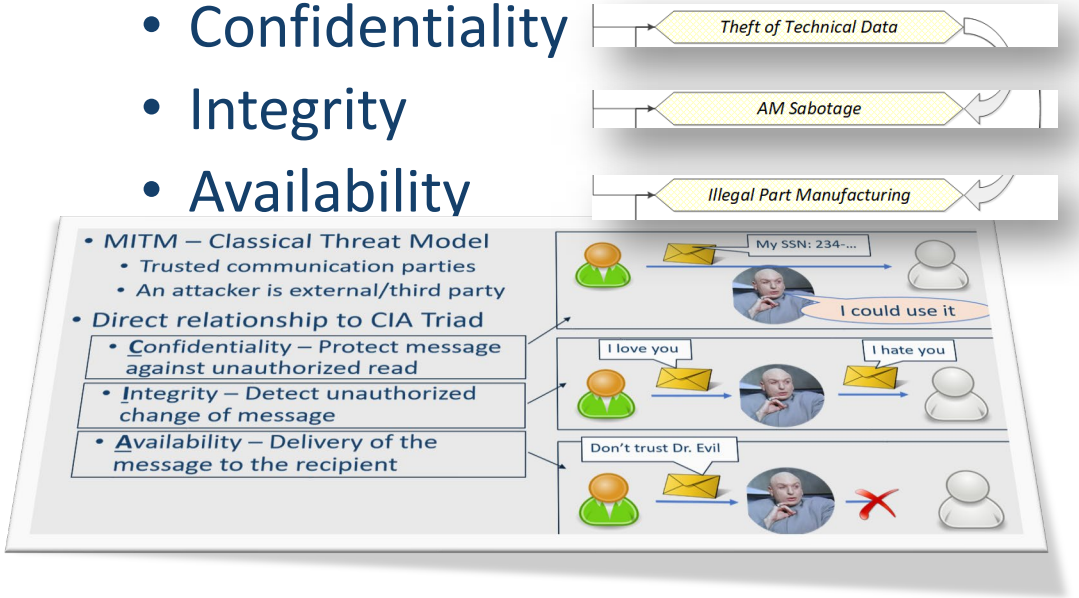
Eric Byres, "The air gap: SCADA's enduring security myth." Communications of the ACM 56, no. 8 (2013): 29-31.

Online: https://dl.acm.org/doi/fullHtml/10.1145/2492007.2492018

Deficiency of CIA Triad in AM

Misconception

- CIA Model directly correlates with AM Security Threats
  - Confidentiality
  - Integrity
  - Availability



Reality in AM

CIA Triad don't relate to AM Security Threats directly

AM Security Threats	CIA Triad C	I	A
Theft of Technical Data	(✓)	✗	✗
Sabotage	✗	(✓)	(✓)
Illegal Part Manufacturing	✗	✗	✗

✓ – Direct correlation, always
(✓) – Correlation in certain cases only
✗ – No correlation at all

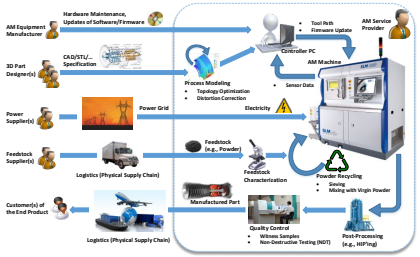
Yampolskiy, M., Gatlin, J., Yung, M. "Myths and Misconceptions in Additive Manufacturing Security: Deficiencies of the CIA Triad." AMSec'21.

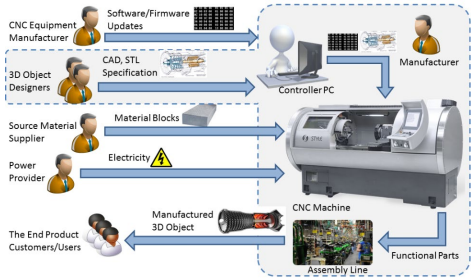
Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING
• Auburn Cyber Research Center (ACRC)
• National Center for Additive Manufacturing Excellence (NCAME)

Reusing Security Solutions

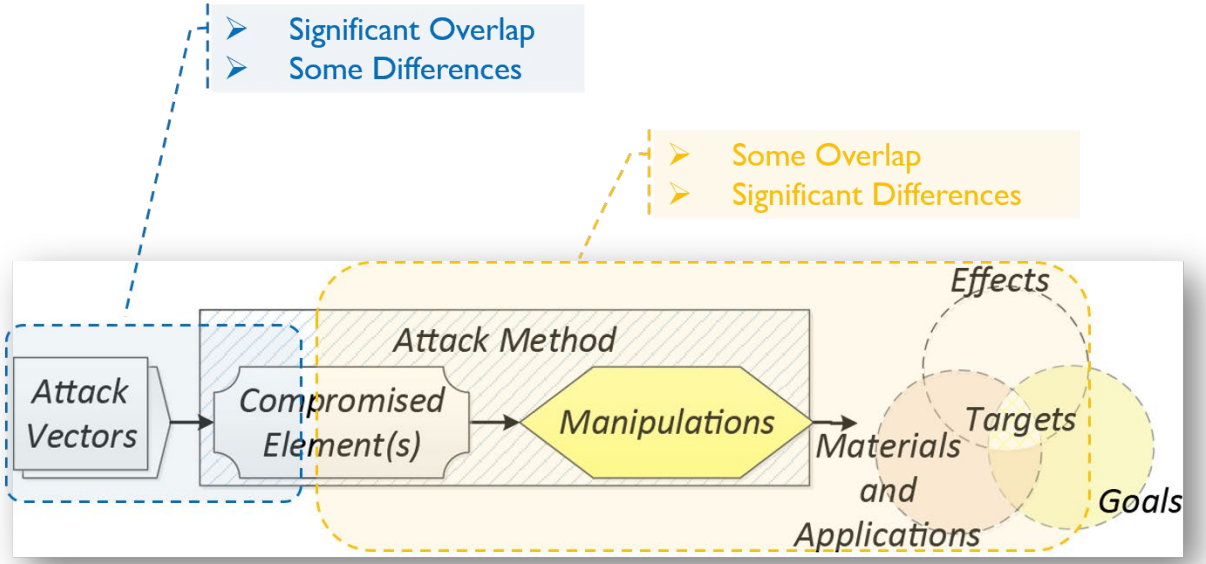
Temptation: Secure AM exactly like other Digital Manufacturing Technologies.

- Comparing Security of AM vs Subtractive Manufacturing with CNC Machines
  - Workflows are somewhat similar
  - Both machines are computerized





- Analysis Results (excerpt):



Graves et al., "Characteristic Aspects of Additive Manufacturing Security From Security Awareness Perspectives." IEEE Access, vol. 7, pp. 103833-103853, 2019. **Available Online:** https://ieeexplore.ieee.org/abstract/document/8779615

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

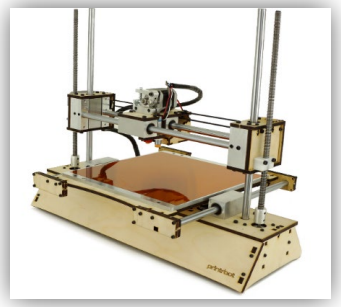
“No 3D Printer was connected to the Ethernet. Only Wi-Fi was enabled.”

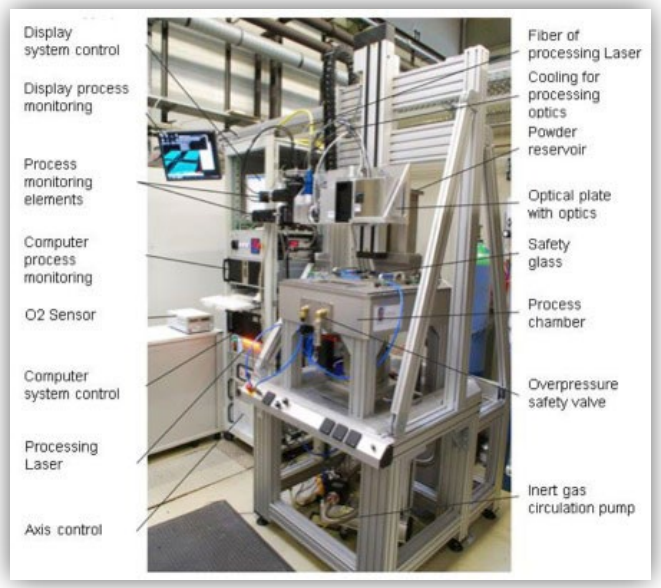
– Undisclosed presentation claiming no Cybersecurity issues identified at AM manufacturer

Final Remarks

Discrepancies: Research & Real Needs

	Current	Needed
3D Printers	Desktop	Industrial-Grade
AM Processes	FDM	PBF, DED
Materials	Polymers	• Metals • Composites





Results from Polymer AM with FDM not always applicable to Metal AM with PBF/DED

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

World Complexity

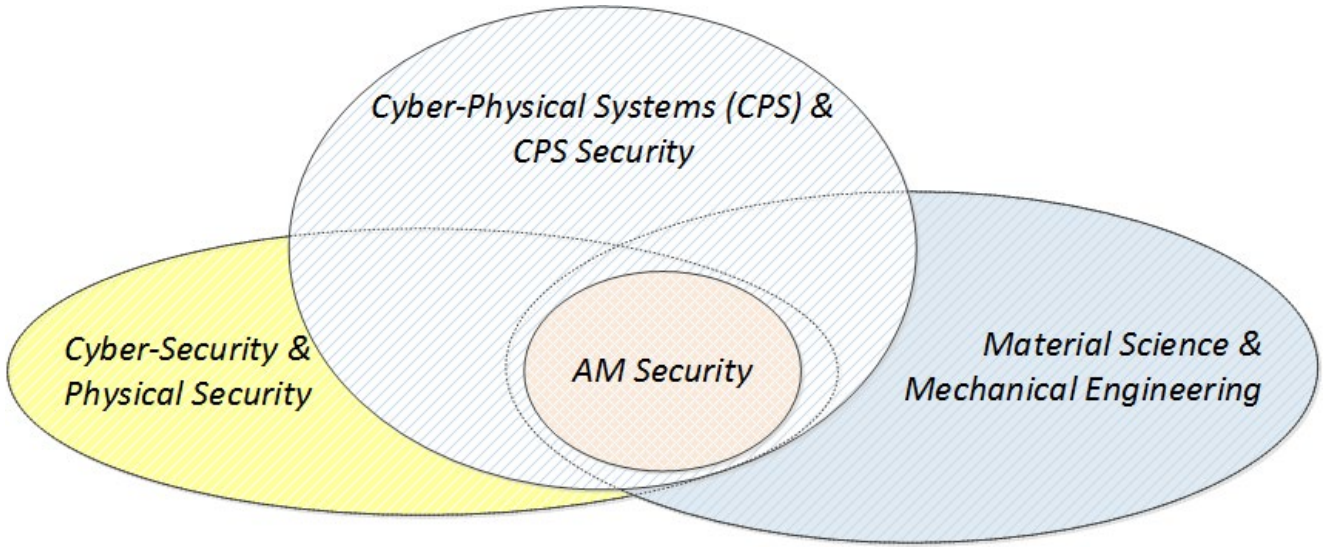
"Universities have departments. The world does not have departments"
– *Richard N. Haass*

Richard N. Haass at "American Foreign Policy: Does it Begin at Home?" talk at Harvard Kennedy School's Institute of Politics

Online on YouTube:
https://www.youtube.com/watch?v=o0dbWdWvR0E&list=TLPQMjcwMzIwMjEHtygQYdrvoQ&index=3

Multi-Disciplinary Field

- *AM Security* is a highly multi-disciplinary research field
  - Can only be solved by **multi-disciplinary** research teams



- **Cyber-Security must be an Integral Part of AM Security**
- **Cyber-Security alone is <u>not</u> Sufficient to Secure AM**

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)
AUBURN UNIVERSITY
SAMUEL GINN
COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

Collaboration Network

Long-Standing

More Recent

Google

COLUMBIA | ENGINEERING
The Fu Foundation School of Engineering and Applied Science

NEW YORK UNIVERSITY

Los Alamos NATIONAL LABORATORY EST. 1943

Georgia Institute of Technology

PURDUE UNIVERSITY

KANSAS CITY NSC National Security Campus

UNSW SYDNEY

Please don't hesitate to reach out if you are interested on collaboration

Dr. Mark Yampolskiy
Computer Science & Software Engineering (CSSE)

AUBURN UNIVERSITY
SAMUEL GINN COLLEGE OF ENGINEERING

- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

The Past and 0ngoing work on AM Security supported by…

Office of Naval Research
Science & Technology
ONR
NIST
America Makes
KANSAS CITY
NSC
National Security Campus

AUBURN UNIVERSITY

Dr. Mark Yampolskiy

- **Samuel Ginn College of Engineering**
- Computer Science & Software Engineering (CSSE)
- Auburn Cyber Research Center (ACRC)
- National Center for Additive Manufacturing Excellence (NCAME)

- **Contact Information**
- e-mail: mark.yampolskiy@auburn.edu