MITRE FiGHT™
Ensuring a Secure & Resilient 5G

Dr. Amir Stephenson, Strategic Outcome Lead, 5G Security
Dr. Michaela Vanderveen, Principal 5G Security Architect

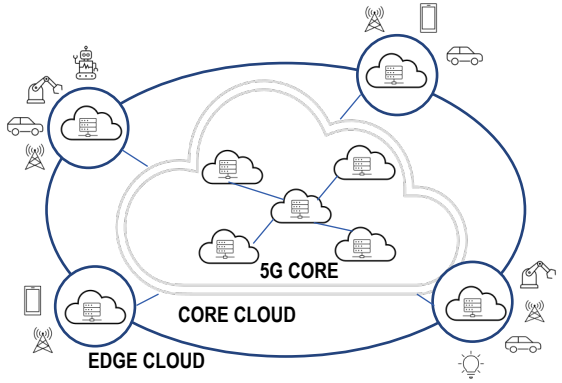
October 2021

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

5G Security: Perspective and Needs

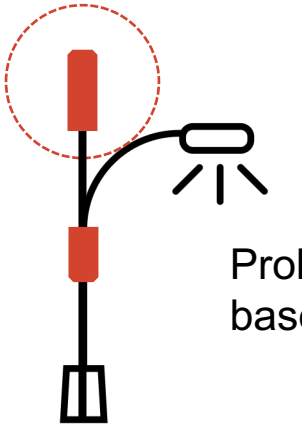
5G is the most secure cellular system to date. However, security vulnerabilities remain.

- The movement towards a service-oriented architecture relying on COTS* presents large attack surface which adversaries will exploit.
- We must be prepared to address emerging and known threats to 5G enabling technology areas



Virtualization and Cloud Usage
(added complexity and security risks)

Supply chain risk



Proliferation of small-cell base stations

By applying a comprehensive 5G Threat Framework to specific use cases and architectures, we can quantify risks and prioritize mitigations to ensure 5G can revolutionize with minimum compromise

*Commercial off the Shelf, including hardware, software, Operating Systems, Infrastructure, etc.

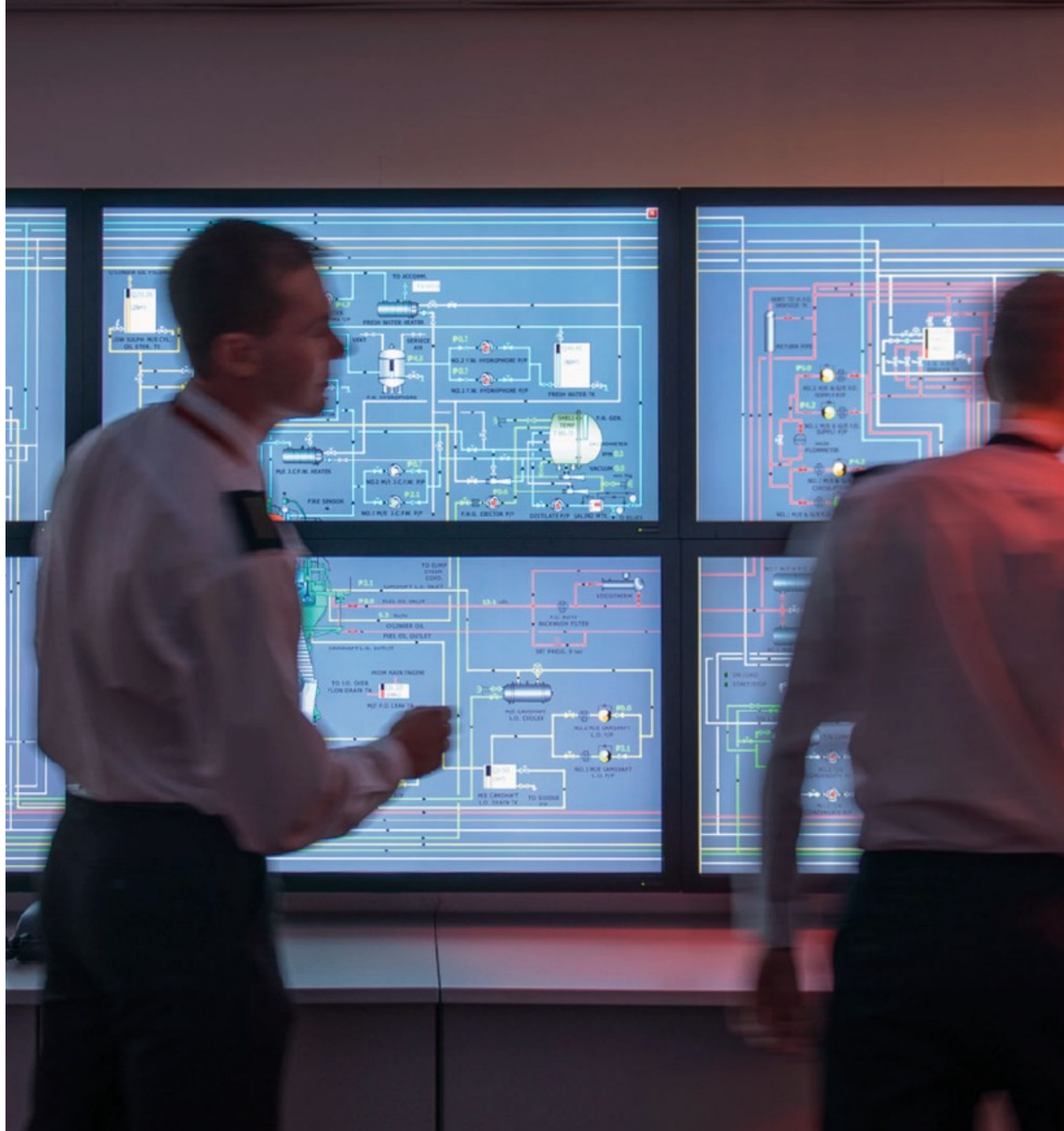
Motivations for a 5G Threat Based Framework

What can the adversary do against U.S. Government (USG) critical assets?

- 5G system well defined: environment bounds adversary operations
- Understanding resulting adversary behavior can inform cyber defense
- Are there weaknesses in the standards?

What can the USG do against the adversary?

- Reduce the attack surface through various mitigations
  - Standards and non-standards based
- Techniques for hunting and removing adversaries from the network



MITRE

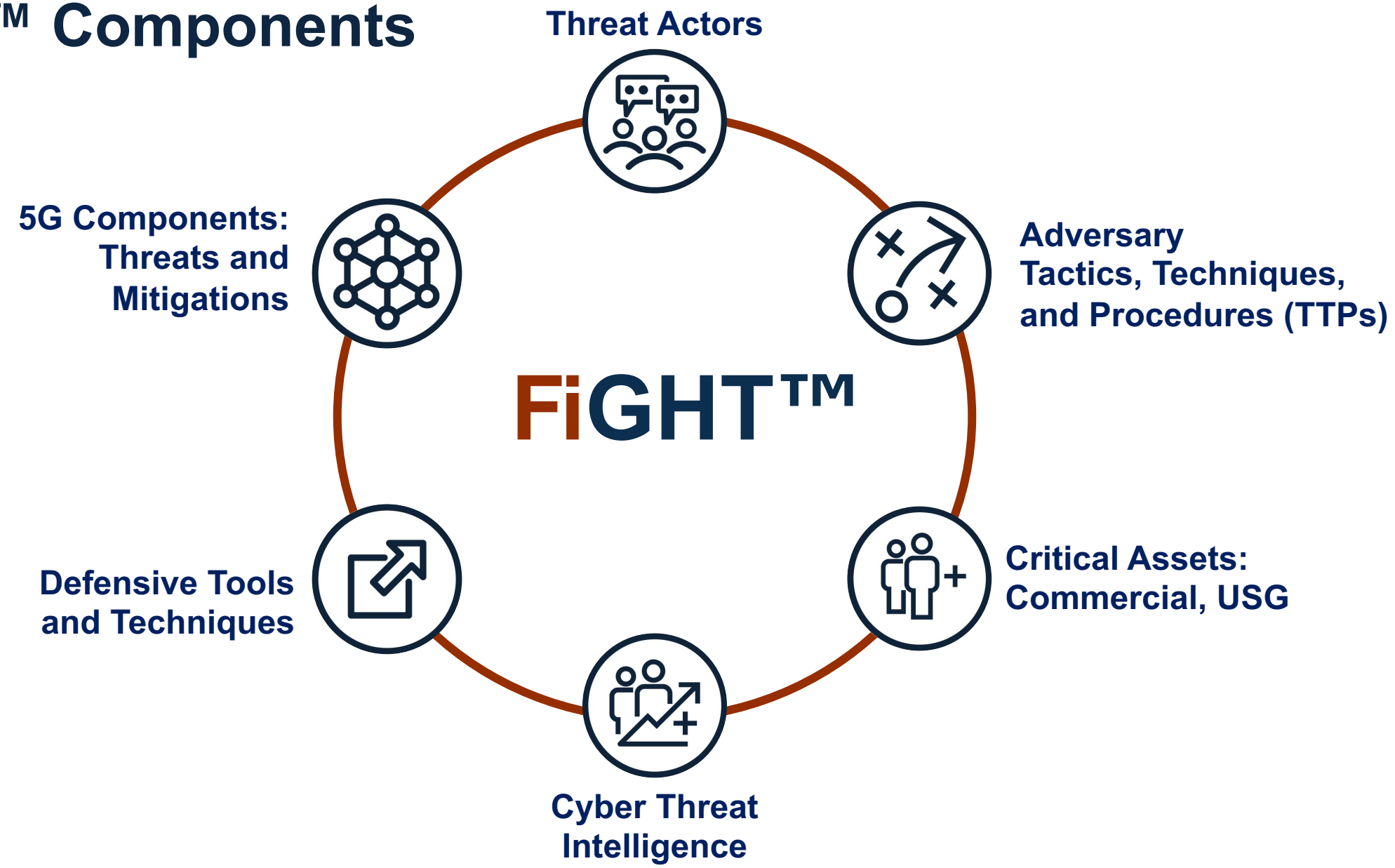
Five-G Hierarchy of Threats

FiGHT™ is a threat-based framework to assess the confidentiality, integrity, and availability of our 5G networks, as well as the devices, weapon systems, and applications using them, for the U.S., and its partners.

FiGHT™ leverages concepts from existing security frameworks and builds upon them by exploring 5G building blocks and the associated hypothesized threats, considering USG critical assets. This enables cyber investment planning and prioritization

FiGHT™ provides a model to assess where 5G cyber investments should be made to achieve the highest impact

FiGHT™ Components



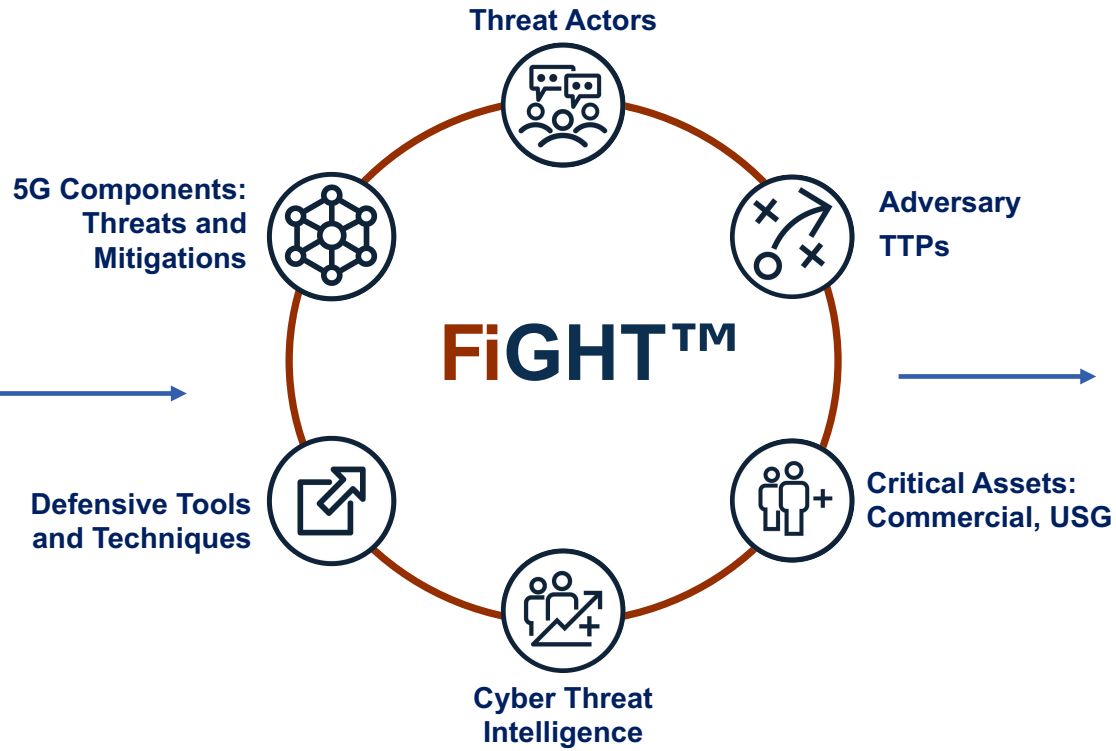
FiGHT™ provides a model to assess what cyber investments should be prioritized

FiGHT™ – Development and Users

MITRE Direct Projects

MITRE Internal Research

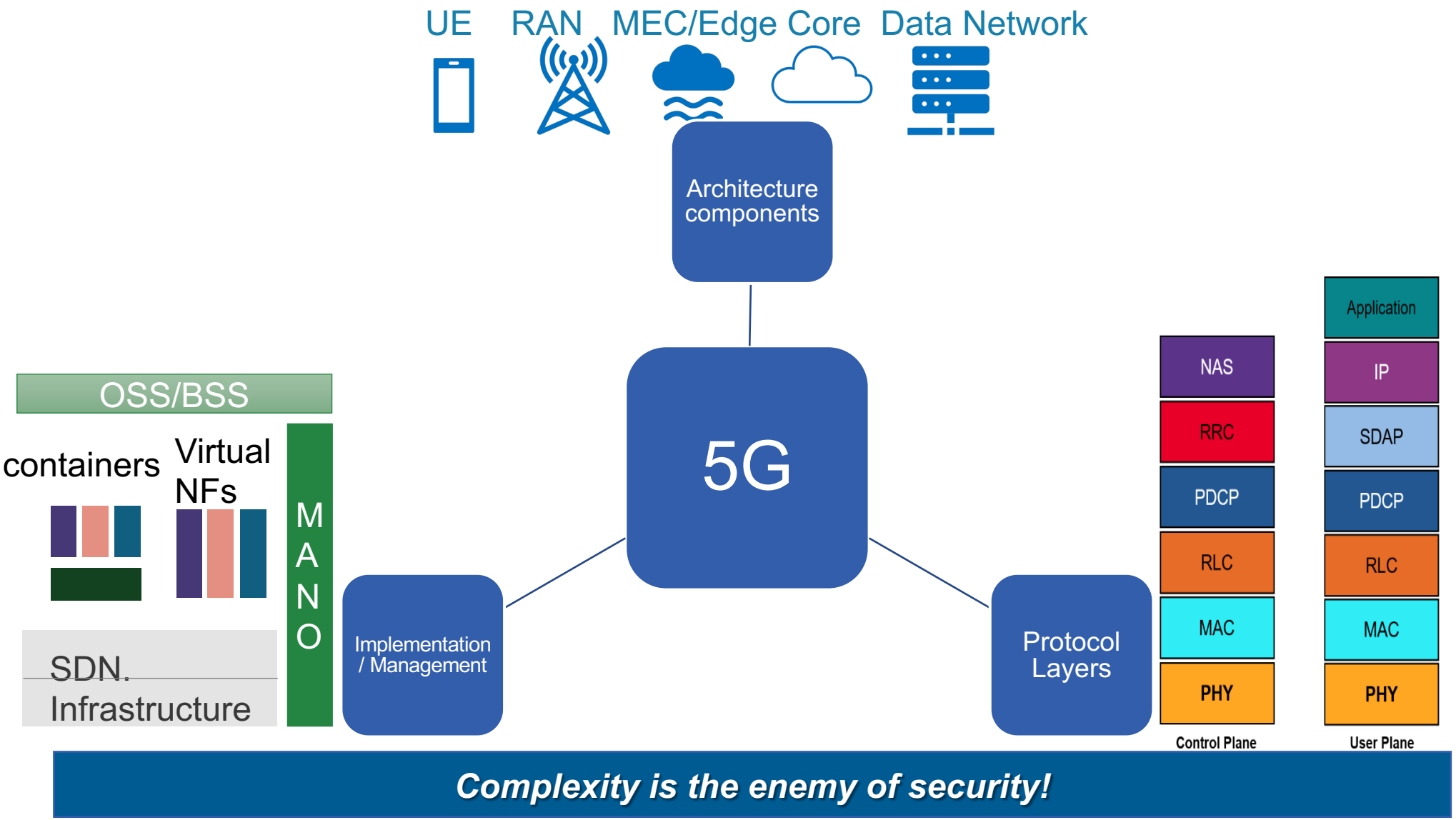
Partnering Opportunities



5G Programs: U.S., and Partners

FiGHT™ can provide structure to mission-specific 5G security assessments and mitigations

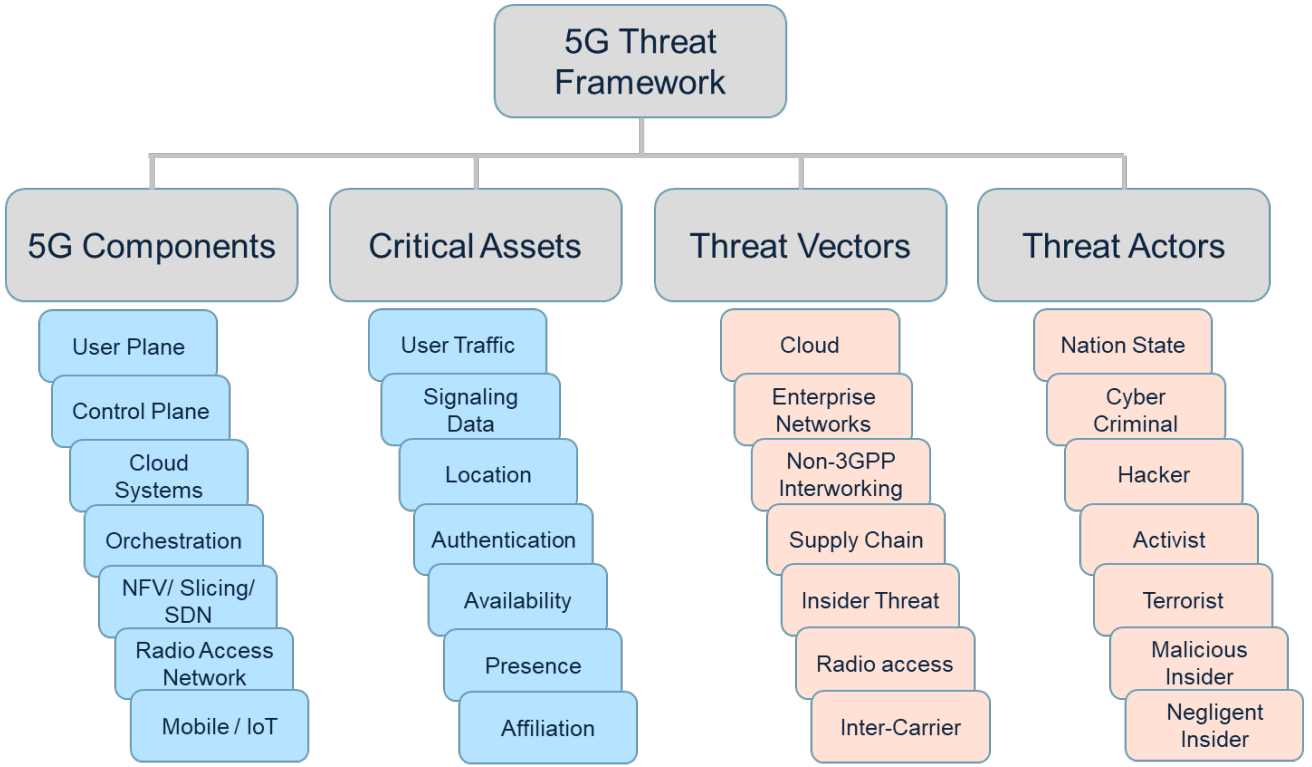
5G: a system of systems



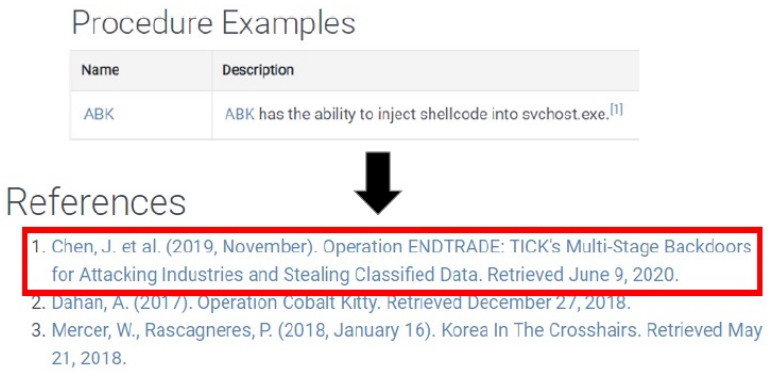
Complexity is the enemy of security!

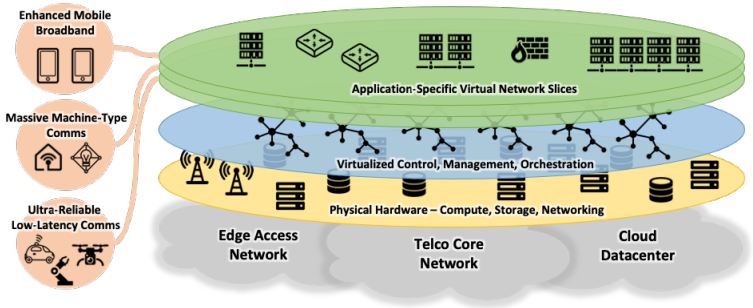
Five-G Hierarchy of Threats (FiGHT™) Framework

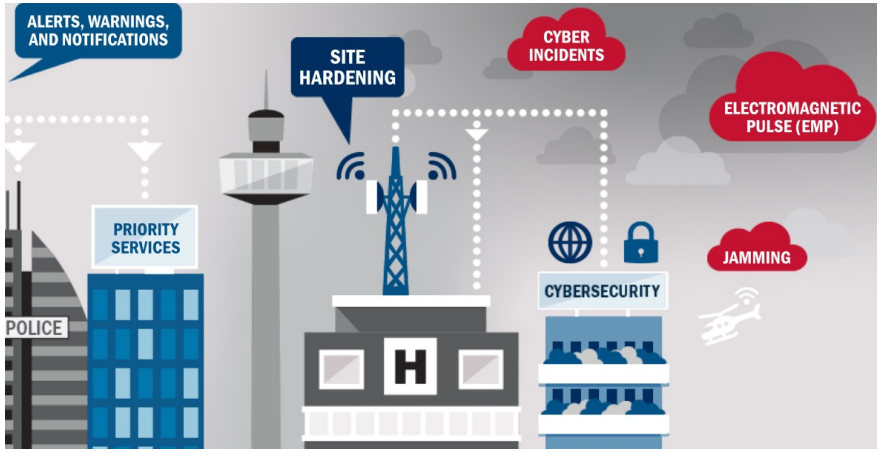
- 5G Components: Building blocks of a 5G System, including inherently cellular technology, and associated technology
  - Analyzed with a security focus
- Critical Assets: What information does the USG need to protect? Where are there differences between the USG's concerns and commercials?
- Threat Vectors: Known threats *(MITRE ATT&CK®)* and emerging threats applicable to 5G
- Threat Actors: Who are the threat actors to 5G systems, and the USGs use of 5G?
  - What are the adversary's goals?



FiGHT™ vs. ATT&CK®







ATT&CK® requires real world observations

A flexible 5G threat-based framework is needed now, not after attacks are observed

ATT&CK® isn't Telecom focused:

Doesn't address all 5G Threats

ATT&CK® for Mobile doesn't include threats to the RAN, Core network, etc.

Doesn't address USG Critical Assets

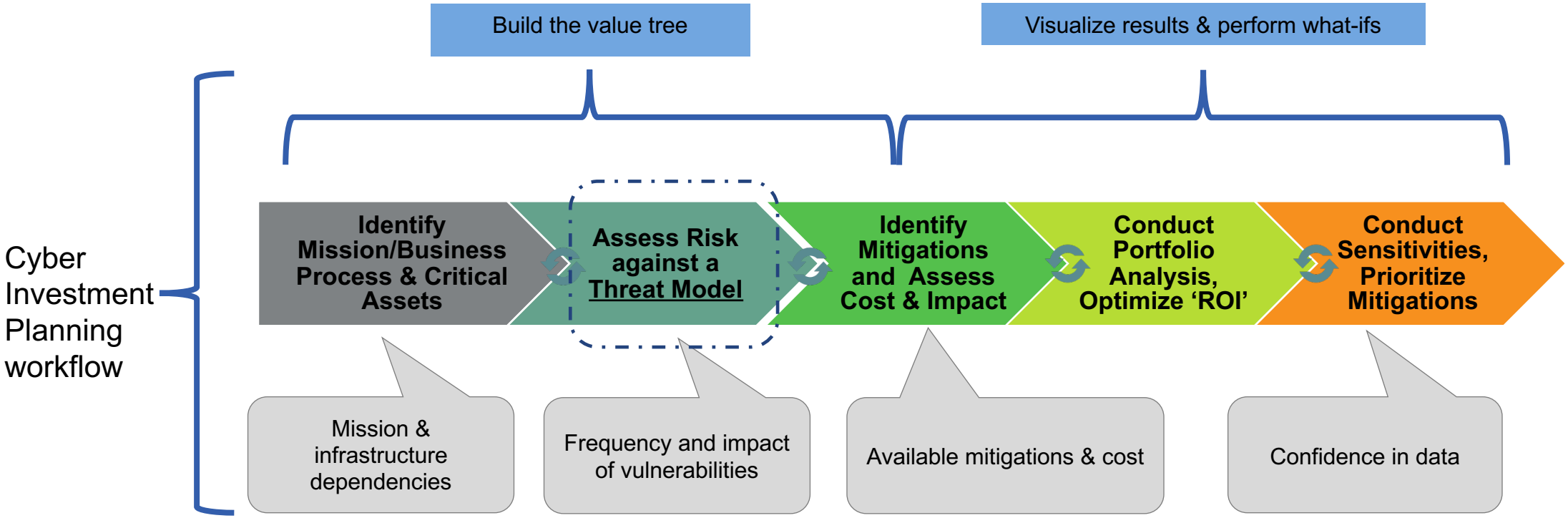
ATT&CK® is focused on adversary TTPs, and doesn't address specific USG requirements associated with telecommunications systems

FiGHT™ leverages concepts and components of ATT&CK®, but is a separate and distinct framework

How will the FiGHT™ Framework be used?

- *Users can leverage FiGHT™ to assess their defenses, emulate adversaries, develop analytics, understand threat coverage, ingest threat intelligence, build threat models, run red team exercises, etc.*
- Identify key connections between critical 5G assets and components with threats and potential mitigations
- Inform Cyber Investment Planning (CIP) to justify prioritization of mitigation investments

FiGHT™ Framework's Role in Cyber Investment Planning



Cyber Investment Planning (CIP) for 5G will enable evidence-driven justification of cyber risk mitigation investments to counter known and emerging threats

FiGHT™ Maturation Plan

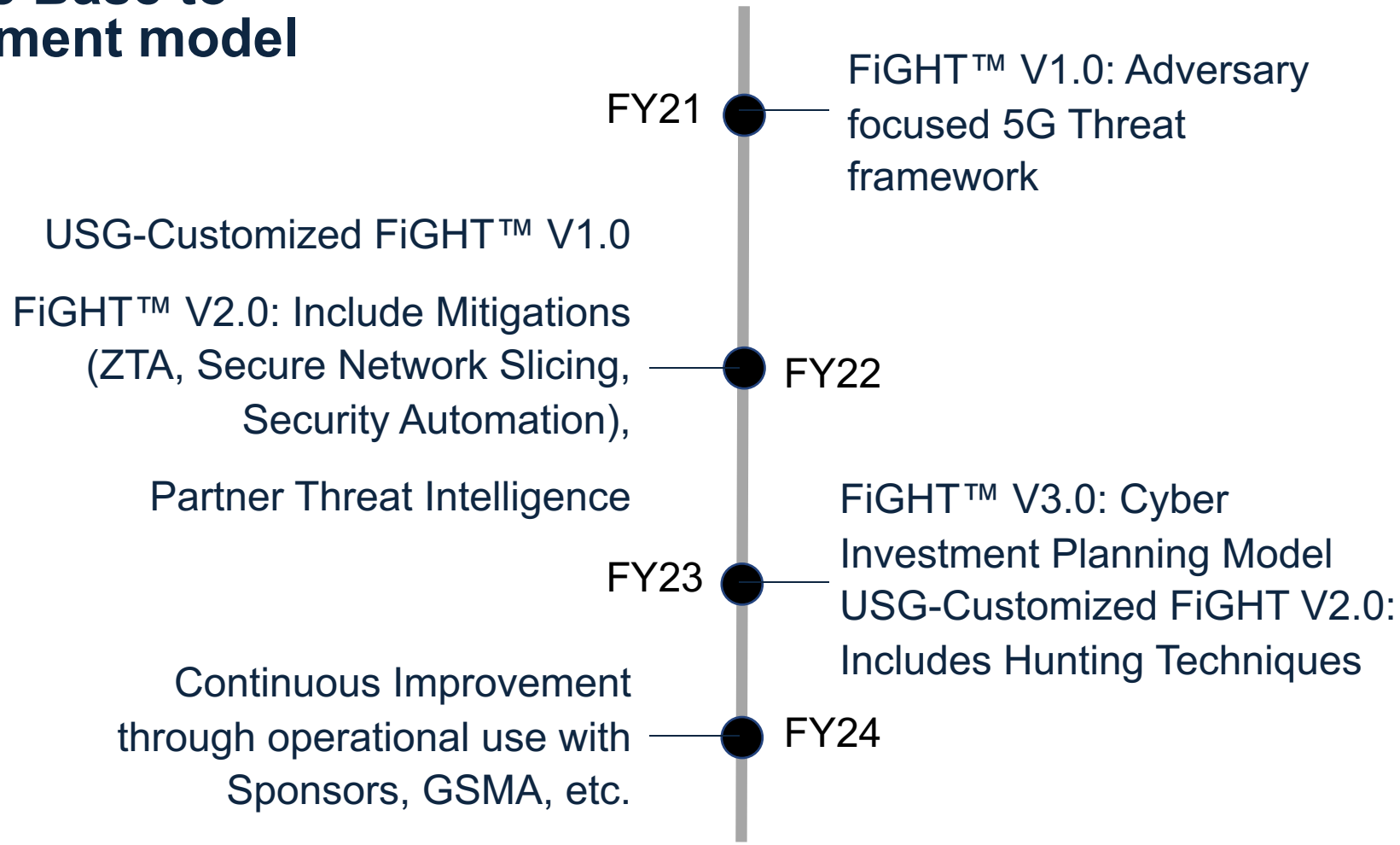
From adversary knowledge Base to functional 5G cyber investment model

FiGHT™ V1.0:

- Built by mapping to existing threat frameworks, conducting literature review of 5G references, and working with university partners on hypothesized threats

FiGHT™ V2.0 and Beyond

- Build upon initial threat framework:
  - Threat Intelligence (Industry Partners, Government)
  - Mitigations (ZTA, Security Automation, Secure Slicing, Operate Through techniques, etc.)



MITRE | FiGHT

Dr. Amir Stephenson

jstephenson@mitre.org

Dr. Michaela Vanderveen

mvanderveen@mitre.org

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™