MITRE

MP230545
MITRE PRODUCT

MITRE FiGHT™: High-Level Overview

MITRE Five-G Hierarchy of Threats (FiGHT)

Project No: OVH010.L100.HFC.J4

McLean, VA

Authors:
Andrew J. Radle
Eric I. Arnoth
Dr. Amir Stephenson
Dr. Michaela Vanderveen
Muddasar S. Ahmed
Dr. Surajit Dey
Adrian Garcia Gonzalez

August 2023

Approved for Public Release; Distribution Unlimited. Public Release Case Number 23-2698

Abstract

MITRE Five-G Hierarchy of Threats (FiGHT™) is a globally accessible knowledge base of adversary tactics and techniques that are used or could be used against 5G networks. These adversary behaviors are based on a combination of theoretical, lab-proven, and real-world observed techniques. FiGHT provides a common taxonomy for both offense and defense, which can be a useful conceptual tool to convey threat intelligence, perform testing through red teaming or adversary emulation, and improve network and system defenses against intrusions. This paper describes the process MITRE used to create FiGHT, the scope of the framework, its relationship to MITRE ATT&CK®, and the approach used for curating new content.

Executive Summary

This paper discusses the creation of FiGHT, a globally accessible knowledge base of adversary tactics and techniques used or potentially used against 5G networks. FiGHT is based on a combination of theoretical, lab-proven, and real-world observed techniques. This paper discusses the components of FiGHT, its design philosophy, and how it can be used. This paper is meant to be used as an authoritative source of information about FiGHT as well as a guide for how FiGHT is maintained and how the FiGHT methodology is applied to the 5G system of systems.

Preface

This paper documents the initial published version of FiGHT as of September 2022. MITRE plans to evolve and expand FiGHT based on industry feedback starting in 2023. This paper will be updated regularly as significant changes are made to FiGHT and the process used to maintain the content within FiGHT.

Trademark Acknowledgments

MITRE ATT&CK® and ATT&CK® are registered trademarks of The MITRE Corporation.

FiGHT™ is a trademark of The MITRE Corporation.

CVE® is a registered trademark of The MITRE Corporation.

CAPEC™ is a trademark of The MITRE Corporation.

STIX™ is a trademark of OASIS Open.

Table of Contents

List of Figures

List of Tables

1 Introduction

The MITRE Five-G Hierarchy of Threats (FiGHT™) is a curated knowledge base that models actual and potential adversary behaviors involved in planning and executing operations against the operators, customers, and suppliers of 5G products, networks, and services. FiGHT is derived from and compatible with MITRE ATT&CK® [1], containing many of the same object sets and mostly following the same schema. Some adversarial behaviors documented in the ATT&CK knowledge base have a special and unique relevance in 5G systems. In these cases, FiGHT directly references these original behaviors and provides additional 5G context that is relevant to the operators and suppliers defending these networks, while also giving a direct link to the source ATT&CK content. FiGHT also has a broader scope for including behaviors, documenting both theoretical and lab-proven predictive (sub-)techniques. This expansion in scope is in addition to adversary behaviors that have been observed in the wild and are documented by either trustworthy cyber threat intelligence (CTI) or shared in confidence by trusted sources. As such, the FiGHT Threat Model can be viewed as a 5G-specific extension and an overlay of ATT&CK.

The FiGHT behavioral model consists of the following core components:

- Tactics that denote the short-term tactical objective of adversaries when performing a specific, atomic behavior
- Techniques that describe the specific, atomic behaviors adversaries perform during an adversary's operation
- Sub-techniques that more specifically describe how a given technique can be achieved, in greater technical detail
- Addendums that provide 5G context for existing ATT&CK objects
- Metadata that captures searchable information about techniques and sub-techniques
- Data sources that can be used by defenders to detect documented techniques and sub-techniques
- Mitigations that can be used by defenders to prevent or minimize the likelihood of adversary success using techniques and sub-techniques

FiGHT is also intended to be a living knowledge base continuously built through community contributions and collaboration. As adversary behavior evolves and 5G progresses to future generations, the FiGHT model will likewise grow to provide an increasingly useful tool for equipment/software developers, operators, service and infrastructure providers, and customers.

1.1 Background and History

The FiGHT framework was created to address a need to understand the potential ways an adversary might compromise 5G networks and to provide defenders with guidance on where and how to mitigate actual and potential adversary behavior. Although the existing ATT&CK model provides a robust foundation for these adversarial use cases, its current scope does not address the needed telecom-specific network aspects. Because 5G stand-alone networks are still in the early stages of deployment around the world, little information is publicly available for adversarial behavior affecting these technologies. Accordingly, there is a difference in scope between FiGHT and ATT&CK frameworks. Currently, ATT&CK is drawn from publicly

reported incidents [2], while FiGHT includes theoretical, predictive behaviors as 5G networks are in the early stages of deployment.

1.2 Mobile Telecommunication Networks Threat Models

FiGHT was created and is being maintained to address the broader 5G scope beyond that addressed by other models. The following list illustrates some of the key differences in coverage between ATT&CK and FiGHT.

- FiGHT will add an addendum to ATT&CK for Enterprise content that has different characteristics in the context of 5G networks, but otherwise remains largely the same.
- FiGHT includes new adversary techniques that do not meet the criteria for inclusion in ATT&CK.
- FiGHT does not duplicate user equipment (UE) threats that are already covered in ATT&CK for Mobile and have no special 5G contextual differences. This is considered out of scope for FiGHT, except for the modem device.
- FiGHT includes coverage for the user device baseband chipset, its interfaces, and software to run on it, all of which are currently out of scope for ATT&CK.
- FiGHT has a set numbering system that is compatible with ATT&CK and does not conflict with the existing index space but can be used to easily trace back original ATT&CK content that is reused in FiGHT.
- FiGHT does not presently document any threats in industrial control systems or other verticals sometimes associated with 5G (e.g., automotive, Internet of Things (IoT)).
- The lack of ATT&CK content in FiGHT should not be seen as indicating it is not relevant to 5G systems, but rather that such existing ATT&CK content is not known to have any special or unique significance in the context of 5G systems. As such, all of ATT&CK may be considered applicable to 5G systems, depending upon specific circumstances.

The way networks are treated between ATT&CK and FiGHT is also different. Because 5G technology is itself intended to provide network services to other entities than the one operating the 5G network, the perspective changes for some techniques and tactics. For example, FiGHT considers the context of denial of service (DoS) and what the adversary accomplishes with DoS techniques. If the result or intent of a DoS attack impacts the availability of the 5G service, i.e., the ability of the UE to connect and send/receive data, then the technique is treated as a network denial of service, FGT1498-Network Denial of Service [3]. By contrast, if a technique impacts the availability of a specific service within the 5G core but the result of such a DoS attack does not prevent UE connection or use of the 5G network, then the technique is treated as a service availability impact, e.g., FGT1499-Endpoint Denial of Service [4].

Error! Reference source not found. is a pictorial representation of the differences between a traditional enterprise network, which is the scope of ATT&CK. **Error! Reference source not found.** is a pictorial representation of a 5G network, the scope of FiGHT, which an MNO builds and operates. These two figures are shown to demonstrate the added complexity inherent in telco industry networks, when compared to a classic enterprise environment that most companies build and operate. In the case of enterprise networks, defenders typically only need to worry about adversaries penetrating their defenses from the Internet, or sometimes as trusted insiders within the organization.

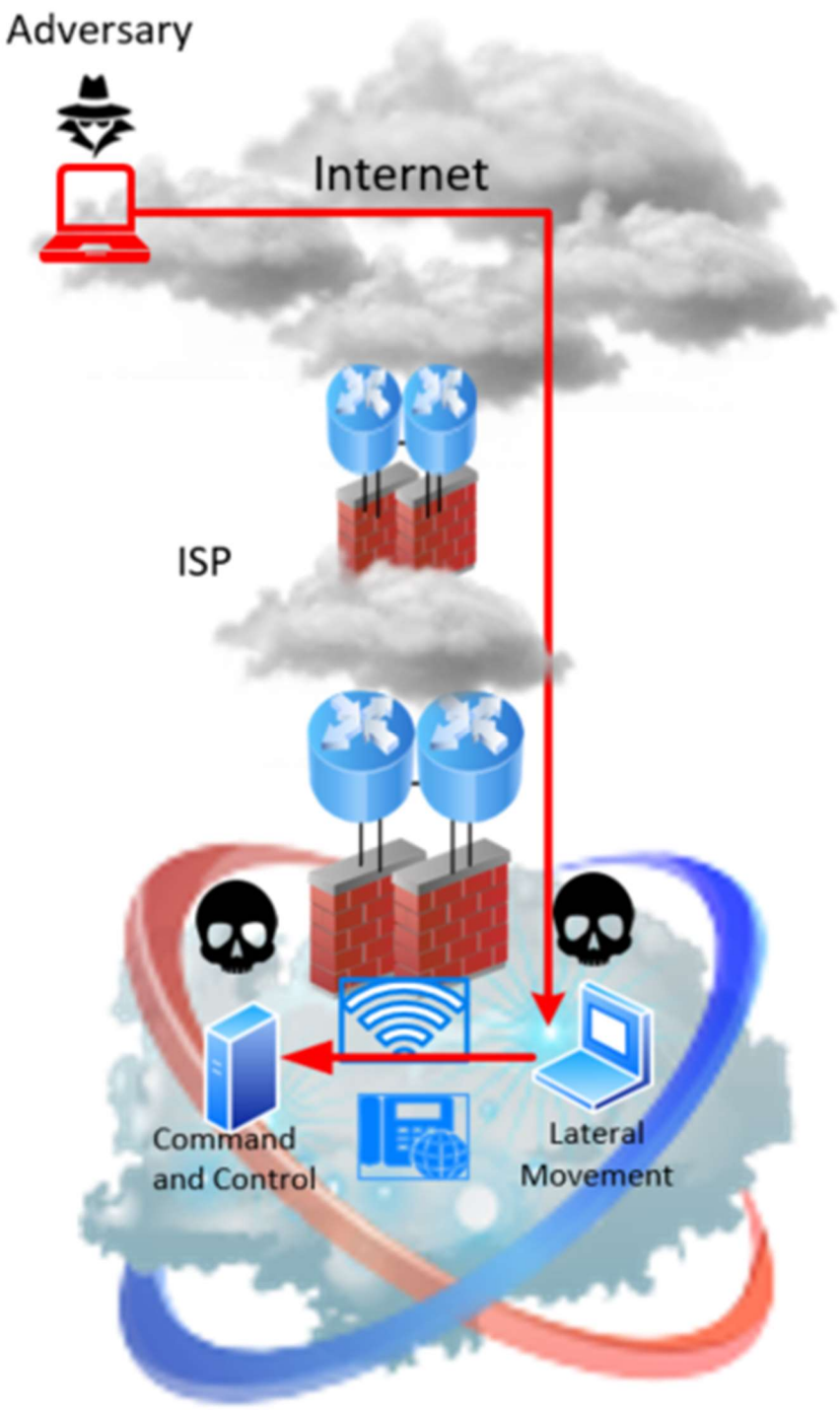

Figure 1 Traditional Enterprise Network

By comparison, MNOs must be aware of not only adversaries from within and without, but also must consider the impact of adversary action directly against their customers, who access 5G networks not from the Internet, but via radio towers with their personal devices. Because the

MNO serves as both telephone operator and Internet Service Provider, while also connecting their 5G network to the Internet, the complexity of interactions between adversaries, mobile user customers, and the MNO's own internal 5G network become very complex very quickly.

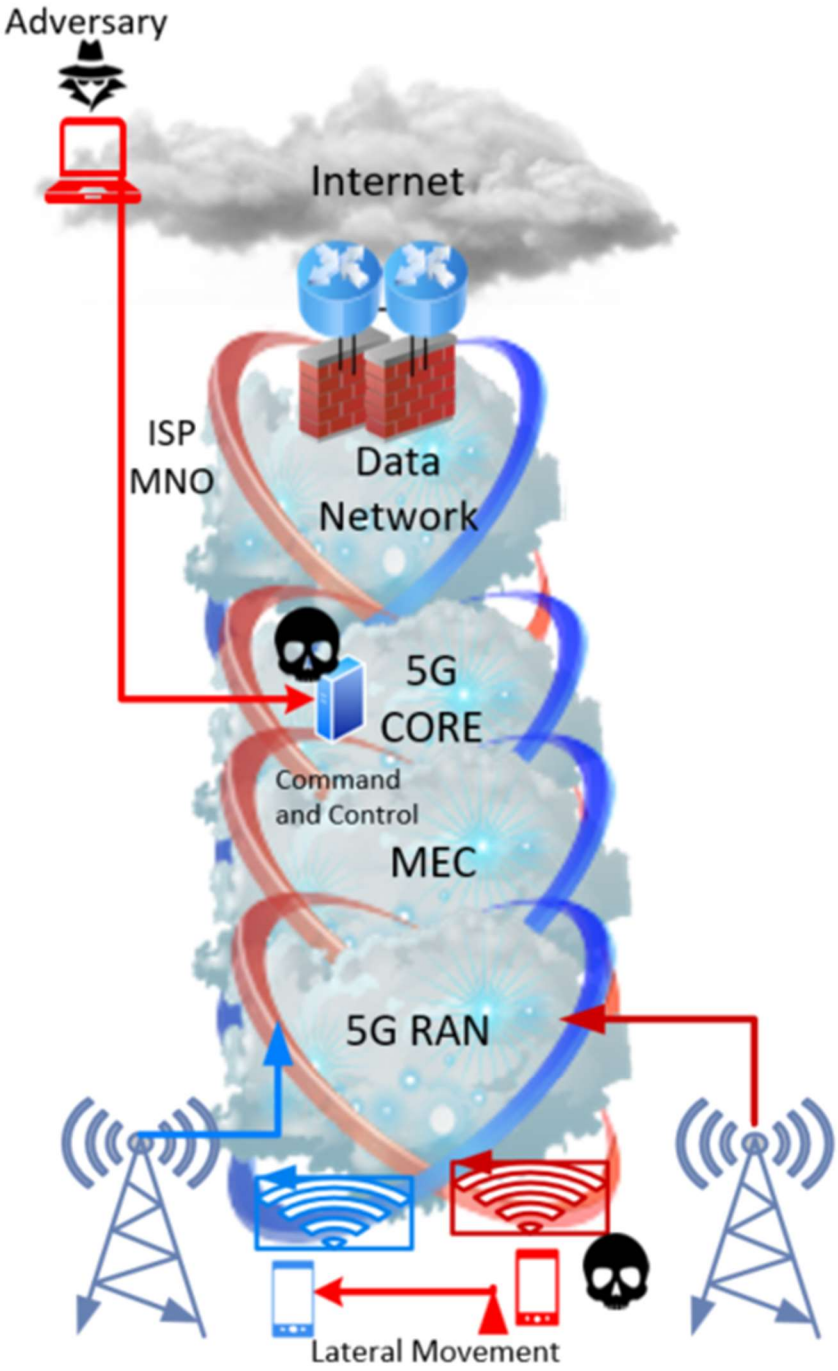

Figure 2 Notional 5G Network

5G also has multiple deployment models and ways to connect to non-5G telecom networks. The model currently includes techniques as follows:

- Technique pertaining to the 5G core network- which employs a service based architecture, unlike earlier generations.
- Techniques pertaining to the radio interface.
- Techniques from earlier generations (3G, 4G) if the technique appears viable in 5G deployments
- Techniques that exploit interconnection and roaming between 5G networks or between 5G networks and earlier generation networks
- Techniques exploiting non-3rd Generation Partnership Project (3GPP) interfaces to 5G
- Techniques from adjacent technologies such as O-RAN and Multi-access Edge Computing (MEC)

The underlying data model and approach can support earlier generation networks, but the focus is on 5G and future generations. The scope may be expanded at a future date to include the earlier, legacy technologies, particularly if the community expresses strong demand and contributes resources to support such enhancements.

2 Potential Users of FiGHT

MITRE currently envisions four primary user groups for the FiGHT framework, though more would be welcome. First, mobile network operators (MNOs) can use FiGHT to better defend against adversaries and detect their activities. Second, many parties can use FiGHT to understand the potential risks posed by adversaries and where mitigations and telemetry may be implemented in their products and services, including 5G equipment vendors, software vendors, and service providers (including cybersecurity, Internet Protocol Exchange [IPX] providers, and cloud services providers), among others. Third, enterprise users of 5G networks and enterprise private 5G capabilities can better assess their deployments, their vendor products, and their associated risks by using FiGHT. Finally, security researchers can use FiGHT to validate techniques, develop new mitigations, and identify additional techniques for inclusion in future versions of FiGHT.

3 Use Cases for FiGHT

The FiGHT framework can be utilized by 5G product/service/solution developers, operators, and users in a variety of ways that further secure deployment, operation, and use of 5G systems. The following security use cases outline some key areas where FiGHT can improve the security of 5G environments.

Defensive Gap Assessment – This may be the primary use case until more 5G networks are deployed and adversary behavior is observed in the wild. This gap assessment helps determine where deployed systems may lack defenses or visibility. The approach can help drive investments when evaluating additional mitigations and product/service acquisitions.

Behavioral Analytics Development – FiGHT can be used to help identify suspicious activity through behavioral analytics. This may be more useful for techniques linked to “seen in the wild” or “proof of concept” activity.

Security Operations Maturity Assessment – The FiGHT framework can be used in conjunction with ATT&CK as a measure of security operations effectiveness at detecting and responding to intrusions. This use case is related to the defensive gap assessment, but is more process focused and can support developing and refining the standard operating procedures and playbooks for responding to detected adversary behavior.

Cyber Threat Intelligence Enrichment – The FiGHT framework can support enriching CTI with the knowledge of adversary group behavior, techniques, and tactics. Due to limited observations of real-world adversary behavior in 5G systems, the CTI process will initially be constrained until more systems are deployed and the enrichment process improved. Use of FiGHT (and ATT&CK) in this way can help guide defensive measures against adversaries mostly likely to target specific operators, suppliers, and service providers.

Adversary Emulation –This is the process of assessing the security of an organization's technology environment by applying CTI about specific adversaries to mimic how they operate. The FiGHT framework can be used to create adversary emulation scenarios and test detection and mitigation approaches that might prevent or detect an adversary's activities.

Red Teaming – This is the process of attempting to breach a defended environment using the same methods and means as an actual adversary. The FiGHT framework can be used to develop red team plans that intentionally attempt to avoid defensive measures that might be in place in a 5G system. The red team can use an adversarial mindset and attempt to apply FiGHT techniques to see what operation impact can be achieved. Since FiGHT also enumerates theoretical and lab-proven techniques, use by a red team can help validate the feasibility and utility of a specific technique.

4 The FiGHT Model

Among other things, FiGHT is a set of techniques that represent actions (behaviors) that adversaries can perform to accomplish short-term objectives. These short-term objectives are represented by the tactic categories. The techniques and sub-techniques under each tactic represent the behaviors that an adversary may use to achieve that tactic. This relatively simple representation attempts to strike a useful balance between sufficient technical detail at the technique level and the context around why actions occur at the tactic level.

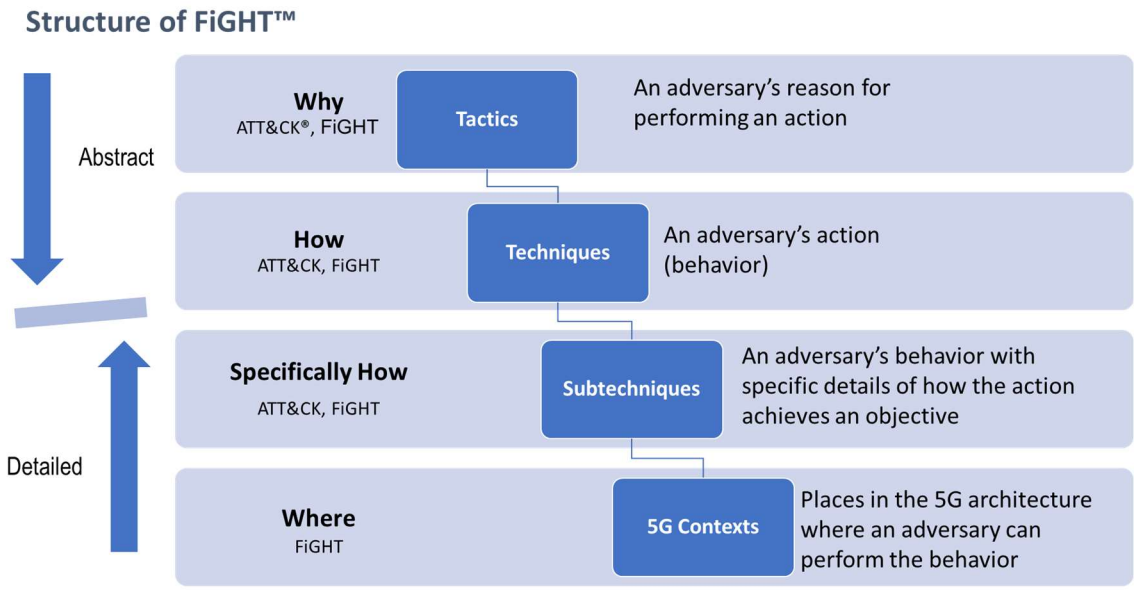

Figure 3 FiGHT Structure

Using an approach between abstract and detailed that MITRE terms mid-tier, FiGHT techniques will generally fall into two levels of abstraction:

- General techniques that apply to multiple platforms in general ways (e.g., Exploit Public Facing Application [5], which depends on vulnerable software)
- General techniques that apply to multiple platforms in specific ways (e.g., Process Injection [6], which has several platform-specific ways it can be done)

Sub-techniques in FiGHT will generally fall into only one level of abstraction:

- A specific way that a technique can be performed that may apply to one or more platforms (e.g., Rundll32 [7] as a specific way to perform System Binary Proxy Execution [8])

4.1 The FiGHT Methodology

The following are the key guiding principles for FiGHT:

- FiGHT always maintains the adversary's perspective.
- Where possible, FiGHT will document the behaviors used by actual adversaries in the wild, where observed and preferably publicly documented through reliable CTI.
- FiGHT documents potential adversary behaviors that are derived from analysis of standards and common design practices, including controlled testing to demonstrate proof of concept.
- FiGHT, like ATT&CK, uses a mid-tier level of abstraction that is appropriate to bridge offensive action with possible defensive countermeasures.

4.1.1 Empirical Inclusion

Whenever possible, FiGHT will favor techniques drawn from publicly reported incidents. To incorporate non-public incidents into FiGHT, MITRE will work with industry to anonymize and sanitize sensitive details. Part of this cleansing is inherent in the abstraction process. Metadata within FiGHT indicates whether a given technique was derived from empirical sources, is proof-of-concept, or is theoretical in nature. Due to sensitivity concerns by a source, any given technique may directly cite a public document or the organization providing the information. Public sources such as threat intelligence reports, conference presentations, non-confidential industry standards body reports, government reports, webinars, blogs, vendor white papers, and social media, among others, are all typical sources of empirical use.

4.1.2 Predictive Techniques

MITRE applies an adversary mindset to the 5G service and often builds theoretical, predictive attack chains to derive theoretical techniques. FiGHT also incorporates proof-of-concept validated techniques. The techniques are tagged to indicate their derivation. Theoretical techniques are those potential adversarial behaviors that have been identified as possible in a particular 5G context to achieve one or more given tactics. For example, exploiting weakness or lack of implementation of authentication tokens to access resources such as sensitive UE data stored in the core network database—such a procedure can be designed using largely 3GPP-spec compliant procedures.

Theoretical techniques are developed through multiple approaches and can be grouped into a few broad categories. In the first approach, existing ATT&CK techniques are analyzed for applicability to 5G systems. In many cases, platforms, architectures, and so on, used for many years in large enterprises are being used for 5G services, and subject matter experts expect adversaries may attempt to use proven techniques against 5G systems. The second approach is analysis of standard and related industry documents that describe how the system should work and where possible areas of concern may exist in the systems built from those standards. The third approach is to develop a notional 5G model system and analyze that system for potential vulnerabilities—places where an adversary might achieve both intermediate and ultimate objectives. This may involve working from the adversary's objective to find a possible entry point, then trying to show whether the model will allow the adversary to work toward that objective. Analyzing the 5G system of systems for weaknesses includes, but isn't necessarily limited to, the following aspects that introduce vulnerabilities and weaknesses in a system:

- Where attack surface exists
- Weaknesses and flaws in the standards, including optional aspects
- Weaknesses carried from prior generations and support for backward compatibility
- Implementation of standards in products/services
- Capacity limitations
- Configuration of products/services
- Process design weaknesses
- Operational practice weaknesses
- User error

4.1.3 Community Collaboration

FiGHT relies heavily on the community, including industry groups like standards bodies, vendors, operators, researchers, test-bed operators, and users, to improve and refine it. This collaboration is not just to identify new techniques but also to improve the utility of FiGHT and how it may be applied by its users. Although FiGHT builds on and is compatible with ATT&CK, MITRE is open to deviations from the ATT&CK scope and approach that make FiGHT more effective and useful to the 5G ecosystem, insofar as these changes do not break backward compatibility with ATT&CK.

As part of this collaboration, the following sources are requested. This is not an exhaustive list, but rather a starting point.

- 5G network operators, including private 5G
- Industry standards and advocacy groups, e.g., GSMA, 3GPP, ETSI
- 5G service providers, including VAS, IPX, infrastructure, and cloud service providers
- 5G equipment and software vendors
- Telecom-focused security researchers and service providers
- Open-source software community supporting 5G
- Cybersecurity service and product providers

Groups and individuals interested in collaborating on FiGHT should visit fight.mitre.org for how to engage with MITRE and the larger FiGHT community. Current options at the time of this document's publication include a dedicated email account and a Slack workspace, which can be found at https://fight.mitre.org/resources/contact. Additional options may be made available in the future and information about these resources will be listed on FiGHT's website.

4.2 Abstraction Levels

Different threat models take different approaches to representing the perceived realities of adversaries and their behaviors and tooling. Some, such as the Lockheed Martin Cyber Kill Chain® [9] and Microsoft's STRIDE [10], are a high level of abstraction, summarizing multiple and complex steps taken by an adversary in a short list of steps. Other models, like CVE® [11], detail low-level concepts, such as detailed system vulnerabilities and exploits that are very specific. The FiGHT framework is a mid-level abstraction model, much like the ATT&CK framework and MITRE CAPEC™ [12]. This mid-level model was chosen due to ATT&CK's proven utility in modeling the behaviors of adversaries, as well as to ensure FiGHT is compatible with the ATT&CK framework.

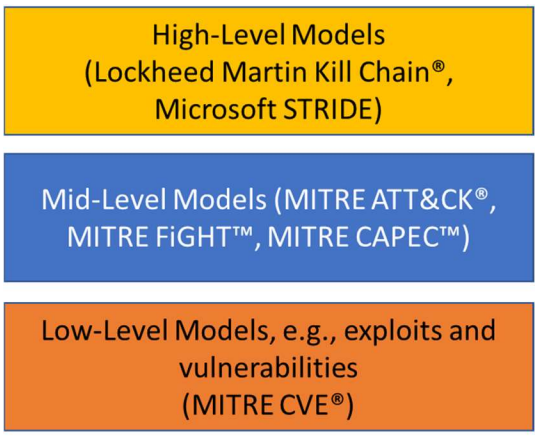

Figure 4 Abstraction Layer Comparison for Different Models

4.3 The FiGHT Matrix

The FiGHT [13] matrix shown in Figure 5 is a visual representation of the relationship between tactics, techniques, and sub-techniques in the FiGHT knowledge base. For example, under the "Initial Access" tactic in FiGHT version 1.0, contains techniques such as "Trusted Relationship," "DNS Manipulation," and "Unauthorized access to Network Exposure Function (NEF) via token fraud" that express ways an adversary can achieve their short-term goal of gaining initial access into an operator environment.

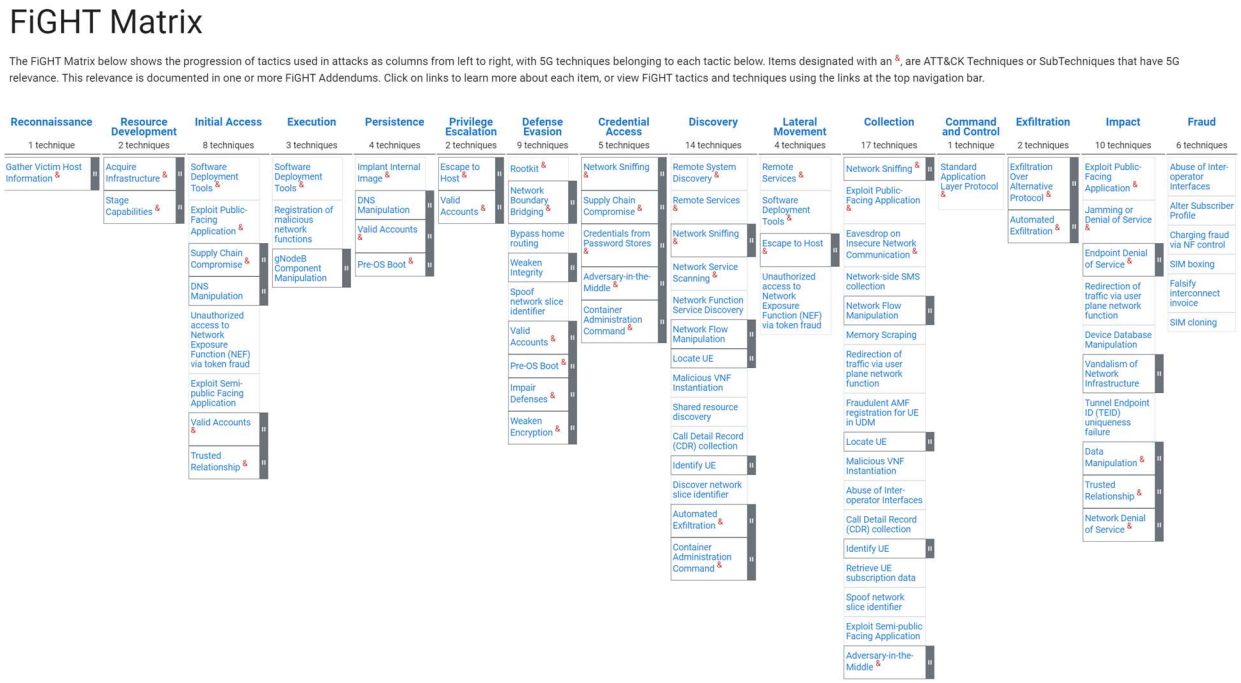

Figure 5 The FiGHT Matrix

Some techniques can be broken down into sub-techniques that describe in more detail how those behaviors can be performed. For example, as of FiGHT version 1.0, "Supply Chain Compromise" has two sub-techniques consisting of "SIM Credential Theft" and "Compromise Service Supply Chain" to describe how "Initial Access" is achieved. Figure 6 depicts the "Initial

Access" tactic with techniques expanded to show sub-techniques. The red "&" shown next to some techniques and sub-techniques in the matrix indicates that the technique or sub-technique is an addendum to an existing MITRE ATT&CK technique or sub-technique.

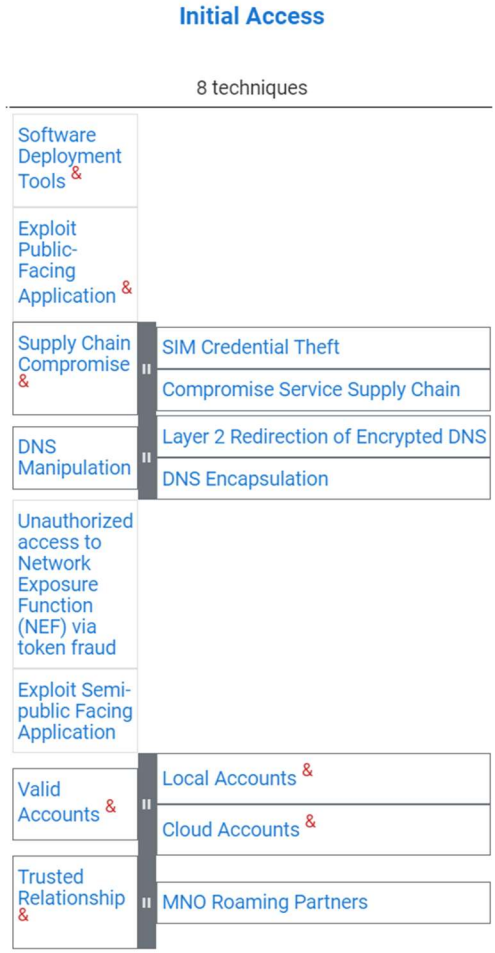

Figure 6 "Initial Access" Tactic (Expanded)

4.4 Tactics

Tactics are why an adversary may perform a given action, and at least one tactic will be listed for each technique. Although a series of adversarial behaviors are ultimately used for achieving campaign-level objectives such as exfiltration of key data, destructive purposes, and so forth, the tactic represents the short-term purpose behind the behavior in question.

Figure 7 FiGHT Tactics

The FiGHT framework includes 15 tactics, which are shown in Figure 7. The size of the bubble is proportional to the number of FiGHT techniques under it. Most of these tactics are commonly seen in enterprise and industrial control systems. FiGHT notably has a "Fraud" tactic; it is focused on service fraud that involves bypassing controls to gain access to services or resources that the adversary is not entitled to or charged for. For example, the adversary may seek to bypass billing and charging fees for use of services provided by an MNO. FiGHT includes this tactic as it is an important area for operators and a key adversary objective for earlier generation networks.

It should be noted that the linear depiction of tactics in the FiGHT matrix are not meant to indicate any corresponding linear sequencing of adversary behaviors during their campaigns to breach 5G networks. When adversaries prepare for a campaign, then execute a campaign, they

may jump from column to column, from technique to technique, with no regard to the linear presentation of these columns and rows in the matrix view.

4.5 Techniques and Sub-Techniques

Techniques, the "How" in **Error! Reference source not found.**, are the atomic behaviors that an adversary may perform when attacking a 5G network. As FiGHT is a mid-level abstraction model, these behaviors are not a detailed accounting of individual steps needed to achieve the adversary's overall outcome.

FIGHT has three broad types of techniques/sub-techniques:

- FiGHT Techniques
  - These are techniques or sub-techniques unique to the FiGHT framework
- FiGHT Sub-techniques
  - These are sub-techniques to an existing FiGHT or ATT&CK technique
- Addendums
  - These are 5G-specific annotations to an existing ATT&CK technique or sub-technique that explain significant details of an adversary behavior that are relevant in the context of a 5G system
  - Addendums have names, but the technique ID will have the same number portion in FiGHT as the ATT&CK ID, e.g., FGT1195 corresponds to T1195, Supply Chain Compromise.
  - An ATT&CK technique may have one or more addendums, depending upon specific 5G contexts.

4.5.1 Platforms

The platform associated with a technique or sub-technique indicates the system an adversary is operating within when utilizing the technique. For FiGHT, this value may indicate operating systems, applications, generation of mobile networks, or other appropriate designations where this technique applies. The platform is a required field.

4.5.2 Architecture Segment

Architecture segments associate techniques with more specific technical areas of a mobile network environment. For example, a technique that applies to the Multi-access Edge Computing (MEC) environment would have MEC listed. The same technique may also be utilized by an adversary in the 5G control plane and so may also list that as well. Architecture segment is a required field, and the default architecture segment is 5G, used when more specific information is not yet available.

4.5.3 Procedure Examples

Procedures, when documented, capture how a particular adversary did a technique based on CTI. For many techniques, there may not be CTI; therefore, they will not have a procedure example. Theoretical techniques may have implementation examples as described in the following section.

The procedure example is an optional field and may not appear on all techniques and sub-techniques. Procedure examples will include a public reference when available.

4.5.4 Implementation Examples

While procedure examples document adversary behavior based on CTI, implementation examples describe approaches that are theoretical and have been proven in the lab to utilize the technique. Theoretical techniques may have a possible example, but not all techniques will have documented examples or have been proven in the lab.

4.5.5 Sub-Technique Details

A FiGHT sub-technique is a more granular form of a technique that describes how an adversary achieves the tactic(s). Sub-techniques describe more details that build upon their parent technique. Not all techniques will have sub-techniques. If a technique has sub-techniques, the technique will list them. The sub-technique will always list its parent technique.

4.5.6 Mitigations

Mitigations represent security concepts and classes of technologies that can be used to prevent a technique or sub-technique from being successfully executed. Notably, mitigations are preventative in nature and don't include detective nor responsive concepts. Many mitigations in FiGHT are drawn from industry practice and additional 5G specific mitigations have been added if available. The mitigation field is an optional field and may not appear in all techniques and sub-techniques.

4.5.7 Pre-Conditions

Pre-conditions listed with a technique describe a set of conditions that might need to exist and/or adversary activities that may precede use of a technique. This field may indicate possible prior techniques without referencing a specific ID, or the field may show particular information, resources, or other things an adversary might need to facilitate successful use of the technique. The pre-conditions field is an optional field and may not appear in all techniques and sub-techniques.

4.5.8 Post-Conditions

Post-conditions listed with a technique describe in some technical detail what the adversary has achieved or plans to achieve in using the technique. It may also indicate, in general, what follow-on techniques may be possible. The post-conditions field is an optional field and may not appear in all techniques and sub-techniques.

4.5.9 Critical Assets

Critical assets are key technical components in the environment that an adversary may target or that are a part of their objective. These assets are related to the technique being utilized. The critical assets field is an optional field and may not appear in all techniques and sub-techniques.

4.5.10 Detections

Detections describe a potential way for the defender to identify and observe the use of a technique by the adversary. Detections describe how to do this with the required data sources. The detections field is an optional field and may not appear in all techniques and sub-techniques.

4.5.10.1 Data Sources

Data sources represent the various subjects/topics of information that can be collected by sensors/logs. The data source field is required for techniques and sub-techniques that have a detection documented.

4.6 FiGHT and ATT&CK Relationship Diagram

In FiGHT, as in ATT&CK, each high-level component is related to other components, e.g., mitigations, in some way. Since FiGHT is complementary to and builds upon ATT&CK, the relationship between the two is more complicated. The diagram in Figure 8 shows a subset of the relationships, while a fuller picture of the relationships and explanations can be found in Appendix A.

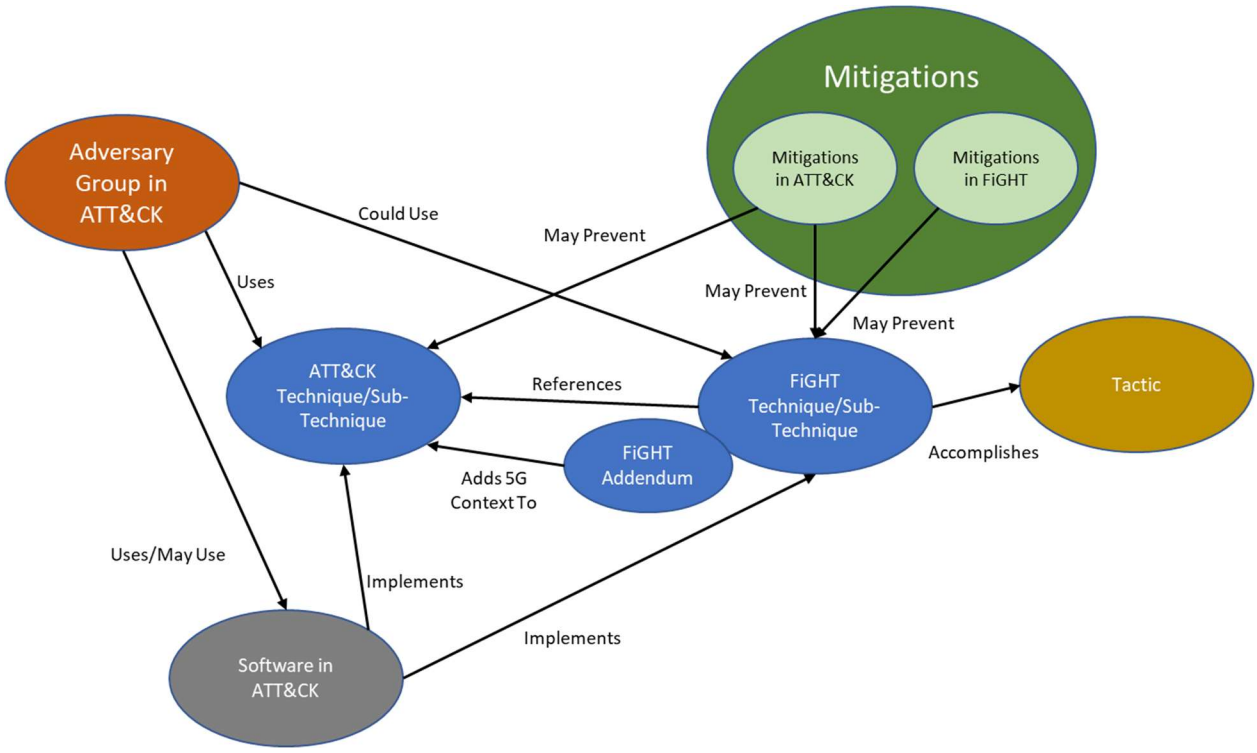

Figure 8 FiGHT Model Relationships (Simplified)

As depicted in the simplified diagram, there will be ATT&CK techniques that do not appear in FiGHT due to the scoping of the FiGHT model today. MITRE anticipates that to fully capture an adversary's attack, the chain of techniques may draw from both ATT&CK and FiGHT. As such, an attack might start inside the enterprise network of an operator using ATT&CK techniques and then move to the network operations and start using techniques that are drawn from ATT&CK but in FiGHT with addendums and pure FiGHT techniques. MITRE has worked to use

compatible labeling, number, and data structures in ATT&CK to enable reuse of tooling, but FiGHT has some extensions to ATT&CK, so complete compatibility may not be possible.

Table 1 FiGHT Model Relationships

Entity	Relationship	Associated Entity	Explanation
Adversary Group in ATT&CK	Could use (predictive)	FiGHT (Sub-) Techniques	If threat actors are using this (sub-) technique, then it's speculated they may use it in 5G platforms.
Adversary Group in ATT&CK	Uses	ATT&CK (Sub-) Techniques	This refers to real-world observations of threat actor behaviors.
Adversary Group in ATT&CK	Uses/May use	Software in ATT&CK	This refers to the tools used by the adversary to conduct their behavior (e.g., commercial code, Operating System (OS) utilities, Free and Open Source Software (FOSS)).
Proven ATT&CK Mitigations	May prevent	ATT&CK (Sub-) Techniques	These represent the security guidance that may prevent an adversary from using a technique.
FiGHT (Sub-) Techniques	References	ATT&CK (Sub-) Techniques	FiGHT references ATT&CK techniques when the ATT&CK technique appears viable in a 5G system.
FiGHT Addendum	Adds 5G context to	ATT&CK (Sub-) Techniques	FiGHT adds context to ATT&CK techniques when the technique may be viable in 5G systems.
Possible Mitigations	May prevent	FiGHT (Sub-) Techniques	These represent possible mitigations that might prevent the adversary from successful use of a (sub-) technique.
FiGHT (Sub-) Techniques	Accomplishes	Tactic	This represents the reason the adversary performs the actions (e.g., reconnaissance, privilege escalation, exfiltration).

4.7 Versioning

The FiGHT framework is published periodically, typically semi-annually, in a series of structured versions. No changes to the threat model are made between minor release versions, and the fight.mitre.org website hosts both the current and all previous versions, either as fully accessible historical sites and/or as an archived copy. With each new release, a changelog is published to show the detailed changes made.

4.7.1 Release Numbers

FiGHT has levels of release numbers, following an X.Y.Z format. Incrementing one of the three number places will indicate the following class of release:

- Major (X): Substantial changes in content and/or model structure to add significant new data or relationships to the framework.
- Minor (Y): Smaller changes in content to incrementally add new data to the framework. No model structure changes.
- Fixes (Z): Updates and corrections due to technical inaccuracies in existing model content. No model structure changes.

The website publishes the version number that tracks the release number in the STIX™ metadata.

4.7.2 Object Deprecation

Objects may be deprecated when they are deemed no longer beneficial to track as part of the knowledge base. This could happen for several reasons, including combining technique ideas together or removing an unnecessary object. Deprecated objects are not deleted from the knowledge base and are still maintained in the STIX repositories, but they no longer show up in the navigation bar and matrix within the main FiGHT website.

5 Summary

This paper discussed the rationale for creating a 5G-focused threat model and described its components, the FiGHT design philosophy, and how it can be used. It is meant to be an authoritative source of information about FiGHT framework, as well as to help guide how FiGHT is maintained.

FiGHT is aimed to be used by mobile network operators, 5G industry vendors, users and researchers and others for initial mitigation, detection of adversary activity, threat hunting, threat intelligence, red teaming, overall risk management, and more. The process of creating and maintaining FiGHT is intended to be transparent and collaborative with the broader community and industry so that users have confidence in the information within it, how it is curated, and how it will be maintained to foster ongoing contributions that will grow it over time with the goal of more secure 5G deployments and services for everyone.

6 References

[1] The MITRE Corporation, "MITRE ATT&CK," [Online]. Available: https://attack.mitre.org. [Accessed 17 October 2022].

[2] The MITRE Corporation, "ATT&CK Design and Philosophy," March 2020. [Online]. Available: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf. [Accessed 8 March 2023].

[3] The MITRE Corporation, "Network Denial of Service," September 2022. [Online]. Available: https://fight.mitre.org/techniques/FGT1498. [Accessed 18 January 2023].

[4] The MITRE Corporation, "Endpoint Denial of Service," September 2022. [Online]. Available: https://fight.mitre.org/techniques/FGT1499. [Accessed 18 January 2023].

[5] The MITRE Corporation, "Exploit Public-Facing Application," September 2022. [Online]. Available: https://fight.mitre.org/techniques/FGT1190/ . [Accessed 12 July 2023].

[6] The MITRE Corporation, "Process Injection," 30 March 2023. [Online]. Available: https://attack.mitre.org/techniques/T1055/. [Accessed 12 July 2023].

[7] The MITRE Corporation, "System Binary Proxy Execution: Rundll32," 21 April 2023. [Online]. Available: https://attack.mitre.org/techniques/T1218/011/. [Accessed 12 July 2023].

[8] The MITRE Corporation, "System Binary Proxy Execution," 18 April 2022. [Online]. Available: https://attack.mitre.org/techniques/T1218/. [Accessed 12 July 2023].

[9] Lockheed Martin Corporation, "The Cyber Kill Chain," [Online]. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. [Accessed 18 October 2022].

[10] P. Garg and L. Kohnfelder, "The Threats To Our Products," Microsoft, 1 April 1999. [Online]. Available: https://shostack.org/files/microsoft/The-Threats-To-Our-Products.docx. [Accessed 18 October 2022].

[11] The MITRE Corporation, "CVE," [Online]. Available: https://www.cve.org/. [Accessed 18 October 2022].

[12] The MITRE Corporation, "CAPEC: Common Attack Pattern Enumeration and Classification," [Online]. Available: https://capec.mitre.org/index.html. [Accessed 18 October 2022].

[13] The MITRE Corporation, "MITRE FiGHT," [Online]. Available: https://fight.mitre.org. [Accessed 17 October 2022].

Appendix A FiGHT Model Object Relationships

The following diagram and table describe, at a high level, the relationship between the components of the FiGHT data model and key elements of the ATT&CK data model.

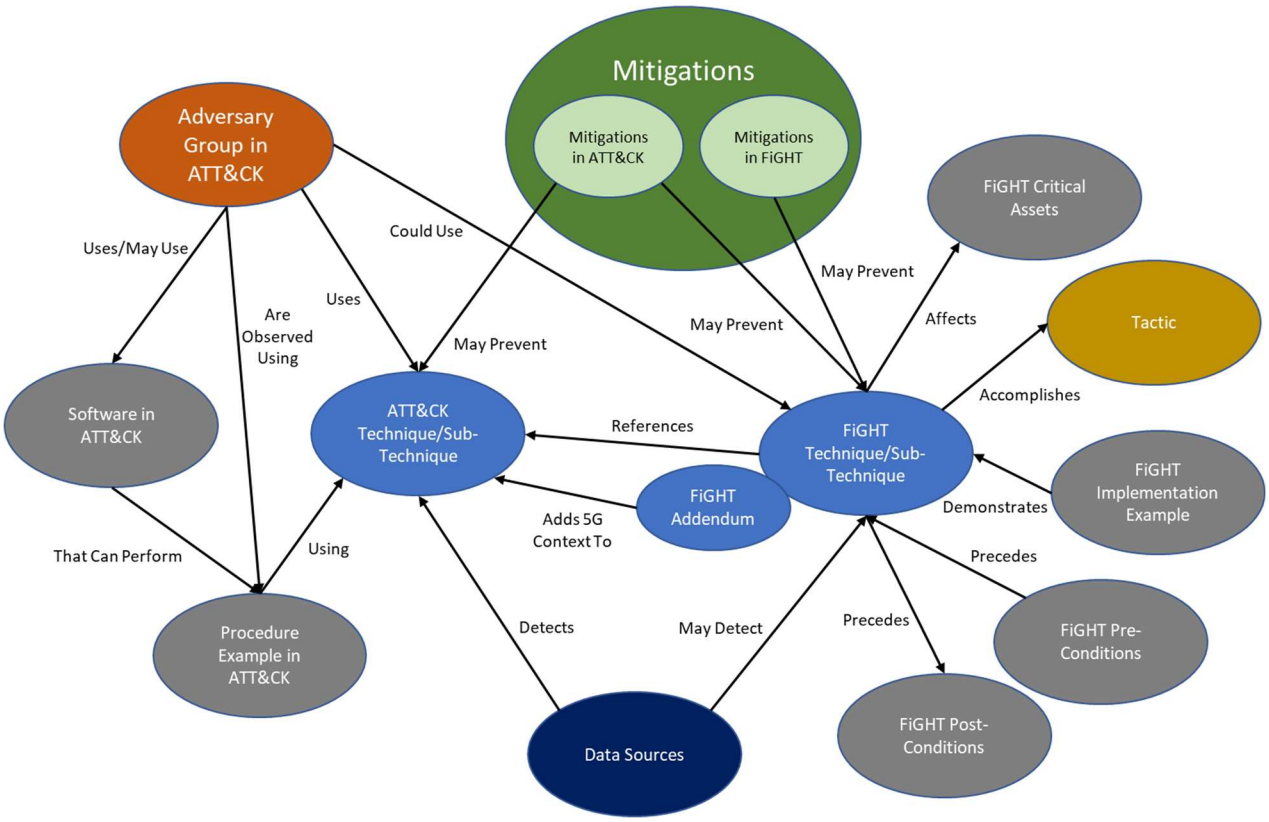

Figure 9 Detailed FiGHT Relationship Model (Comprehensive)

Table 2 Detailed FiGHT Relationship Model

Entity	Relationship	Associated Entity	Explanation
Adversary Group in ATT&CK	Could use (predictive)	FiGHT (Sub-) Techniques	If threat actors are using this (sub-) technique, then it is possible that they could use it in 5G platforms.
Adversary Group in ATT&CK	Uses	ATT&CK (Sub-) Techniques	This refers to real-world observation of threat actor behaviors.
Adversary Group in ATT&CK	Uses/May use	Software in ATT&CK	This refers to the tools used by the adversary to conduct their behavior (e.g., commercial code, OS utilities, FOSS).

Entity	Relationship	Associated Entity	Explanation
Proven ATT&CK Mitigations	May prevent	ATT&CK (Sub-) Techniques	These represent the security guidance that may prevent an adversary from using a technique.
FiGHT (Sub-) Techniques	References	ATT&CK (Sub-) Techniques	FiGHT references ATT&CK techniques when the ATT&CK technique appears viable in a 5G system.
FiGHT Addendum	Add 5G context to	ATT&CK (Sub-) Techniques	FiGHT adds context to ATT&CK techniques when the technique may be viable in 5G systems.
Data Sources	Detects	ATT&CK (Sub-) Techniques	This refers to the logs and sensors that are relevant for threat hunting and intrusion detection.
FiGHT (Sub-) Techniques	Affects	FiGHT Critical Assets	Adversary use of a technique can impact key 5G architectural components and operations.
Possible Mitigations	May prevent	FiGHT (Sub-) Techniques	These are possible mitigations that might prevent the adversary from successful use of a (sub-) technique.
Data Sources	May detect	FiGHT (Sub-) Techniques	This refers to the logs and sensors that are relevant for threat hunting and intrusion detection in a 5G system.
FiGHT (Sub-) Techniques	Accomplishes	Tactic	This represents the reason the adversary performs the actions (e.g., reconnaissance, privilege escalation, exfiltration).
FiGHT Implementation Example	Demonstrates	FiGHT (Sub-) Techniques	This is a summary that suggests how an adversary could implement the technique in the 5G system.
FiGHT Pre-Conditions	Precedes	FiGHT (Sub-) Techniques	These are known pre-conditions that must be in place by the adversary prior to use of a technique.
FiGHT (Sub-) Techniques	Precedes	FiGHT Post-Conditions	These are expected adversarial conditions or activities that may follow

Entity	Relationship	Associated Entity	Explanation
			the application of the technique.
Adversary Group in ATT&CK	Could use (predictive)	FiGHT (Sub-) Techniques	If threat actors are using this (sub-) technique, then it is speculated this is feasible for 5G platforms.
Adversary Group in ATT&CK	Uses	ATT&CK (Sub-) Techniques	This refers to real-world observation of threat actor behaviors.
Adversary Group in ATT&CK	Are observed using	Procedure Examples in ATT&CK	This refers to the details of how a technique is used.
Adversary Group in ATT&CK	Uses/May use	Software in ATT&CK	This refers to the tools used by the adversary to conduct their behavior (e.g., commercial code, OS utilities, FOSS).
ATT&CK (Sub-) Techniques	May prevent	Mitigations	These represent the security guidance that can be used to prevent a technique.
FiGHT (Sub-) Techniques	References	ATT&CK (Sub-) Techniques	This represents relevant complementary adversarial behaviors observed in ATT&CK.
ATT&CK (Sub-) Techniques	Add 5G context to	FiGHT Addendum	Each overlapping ATT&CK technique was enhanced by adding potential 5G risk perspective.
ATT&CK (Sub-) Techniques	Detects	Data Sources	This refers to the logs and sensors that are relevant for threat hunting and intrusion detection.
FiGHT (Sub-) Techniques	Affects	FiGHT Critical Assets	Each adversarial behavior can impact key 5G architectural components and operations.
FiGHT (Sub-) Techniques	May prevent	Mitigations	These represent the security guidance that can be used to prevent a technique.
FiGHT (Sub-) Techniques	May detect	Data Sources	This refers to the logs and sensors that are relevant for threat hunting and intrusion detection.
FiGHT (Sub-) Techniques	Accomplishes	Tactic	This represents the reason the adversary performs the actions (e.g.,

Entity	Relationship	Associated Entity	Explanation
			reconnaissance, privilege escalation, exfiltration).
FiGHT (Sub-) Techniques	Demonstrates	FiGHT Implementation Example	This summary explains how each adversarial behavior could impact 5G systems.
FiGHT (Sub-) Techniques	Precedes	FiGHT Pre-Conditions	These conditions need to exist for the adversary to use this technique.
FiGHT (Sub-) Techniques	Follows	FiGHT Post-Conditions	This is the system's state after an adversary's use of a technique.

Appendix B Terms

Acronym	Definition
3GPP	3rd Generation Partnership Project
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
CAPEC	Common Attack Pattern Enumeration and Classification
CTI	Cyber Threat Intelligence
CVE	Common Vulnerabilities and Exposures
DNS	Domain Name System
DoS	Denial of Service
ETSI	European Telecommunication Standards Institute
FiGHT	Five-G Hierarchy of Threats
FOSS	Free and Open-Source Software
GSMA	Global System for Mobile Communications Association
IoT	Internet of Things
IPX	Internet Protocol Exchange
MEC	Multi-access Edge Computing
MNO	Mobile Network Operator
NEF	Network Exposure Function
OS	Operating System
SIM	Subscriber Identity Module
STIX	Structured Threat Information eXpression
UE	User Equipment