

REPORT DOCUMENTATION PAGE*Form Approved
OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE (DD-MM-YYYY)		2. REPORT TYPE		3. DATES COVERED (From - To)	
4. TITLE AND SUBTITLE				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER (Include area code)

MITRE FiGHT™

Ensuring a Secure & Resilient 5G

June 16, 2023

Contact: Michaela Vanderveen
mvanderveen@mitre.org

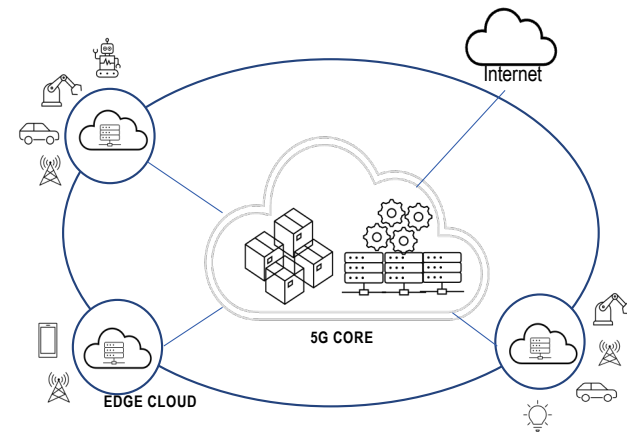
Approved for Public Release. Case Number 23-1945

MITRE | SOLVING PROBLEMS
FOR A SAFER WORLD™

5G Security: Perspective and Needs

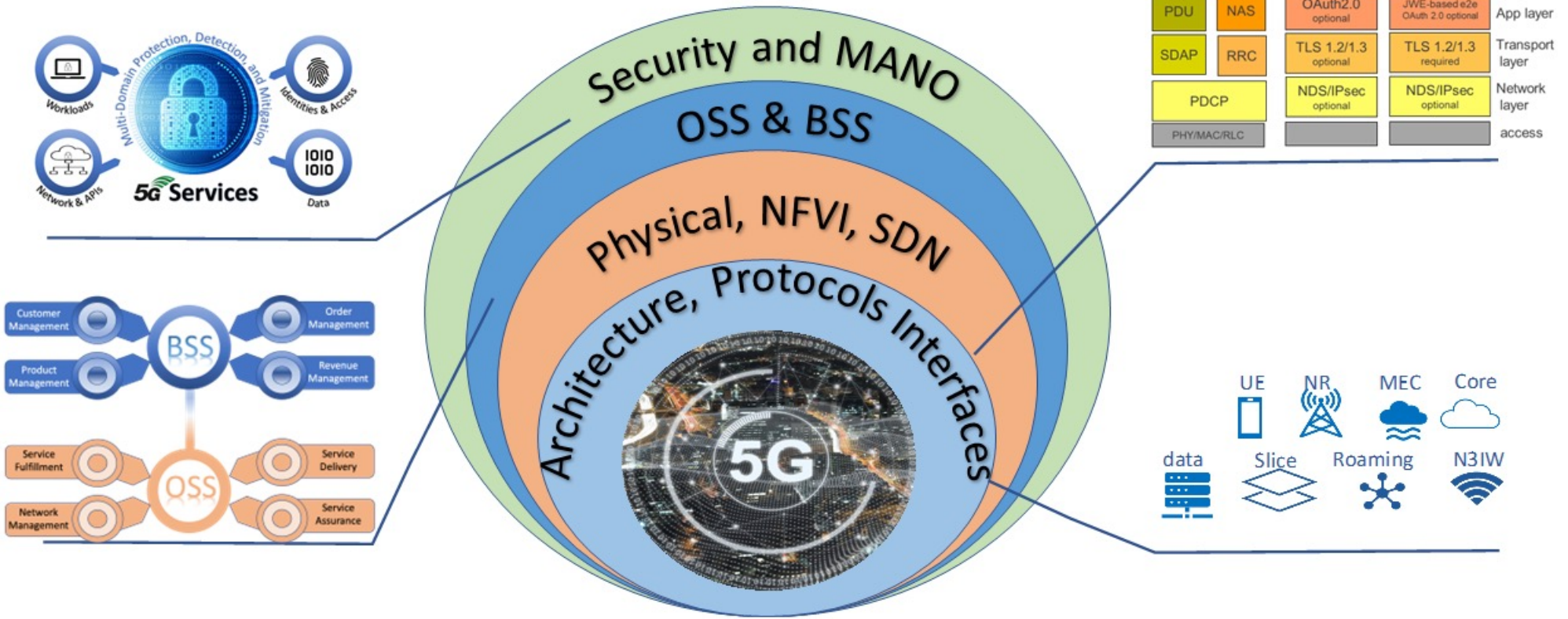
5G is the most secure cellular system to date. However, security vulnerabilities remain.

- Decoupling of software and hardware/platform requires new and additional security measures
- Auxiliary technologies from the Internet are brought into 5G and their threats inherited
- Complexity of deployments (cloud, physical, hybrid) poses a configuration/responsibility challenge
- Supply Chain risk is increasing. Use of COTS* and Open-source s/w is ubiquitous
- Standards (e.g. 3GPP) leave some controls optional



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

5G Complexity: A system of many systems



Complexity is the enemy of security

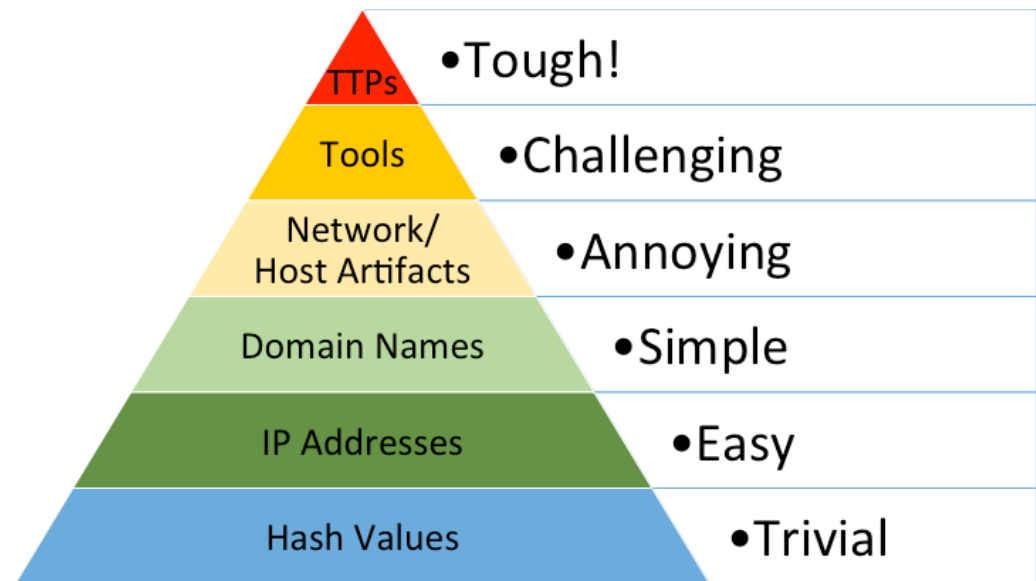
Motivations for a 5G Threat Based Framework

What can the adversary do against your critical assets?

- 5G system well defined: environment bounds adversary operations
- Understanding resulting adversary behavior can inform cyber defense

What can you do against the adversary?

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



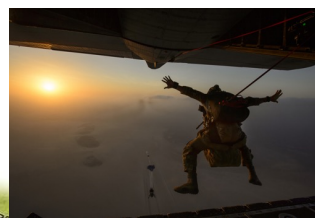
[The Pyramid of Pain](#) by [David J Bianco](#)

Cybersecurity should be *threat-informed*

Knowledge of my adversary can help me answer...

What do I know about my own strengths and weaknesses?

What do I know about my adversary's capabilities and intent?



Reference: [Engineering-as-a-Moat](#)



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 systems and applications using them.

FiGHT™ leverages concepts from existing security frameworks and builds upon them, incorporating predictive and lab-proven threats to critical 5G assets.

Risk Management



Identification



Assessments
Analysis & Prioritization

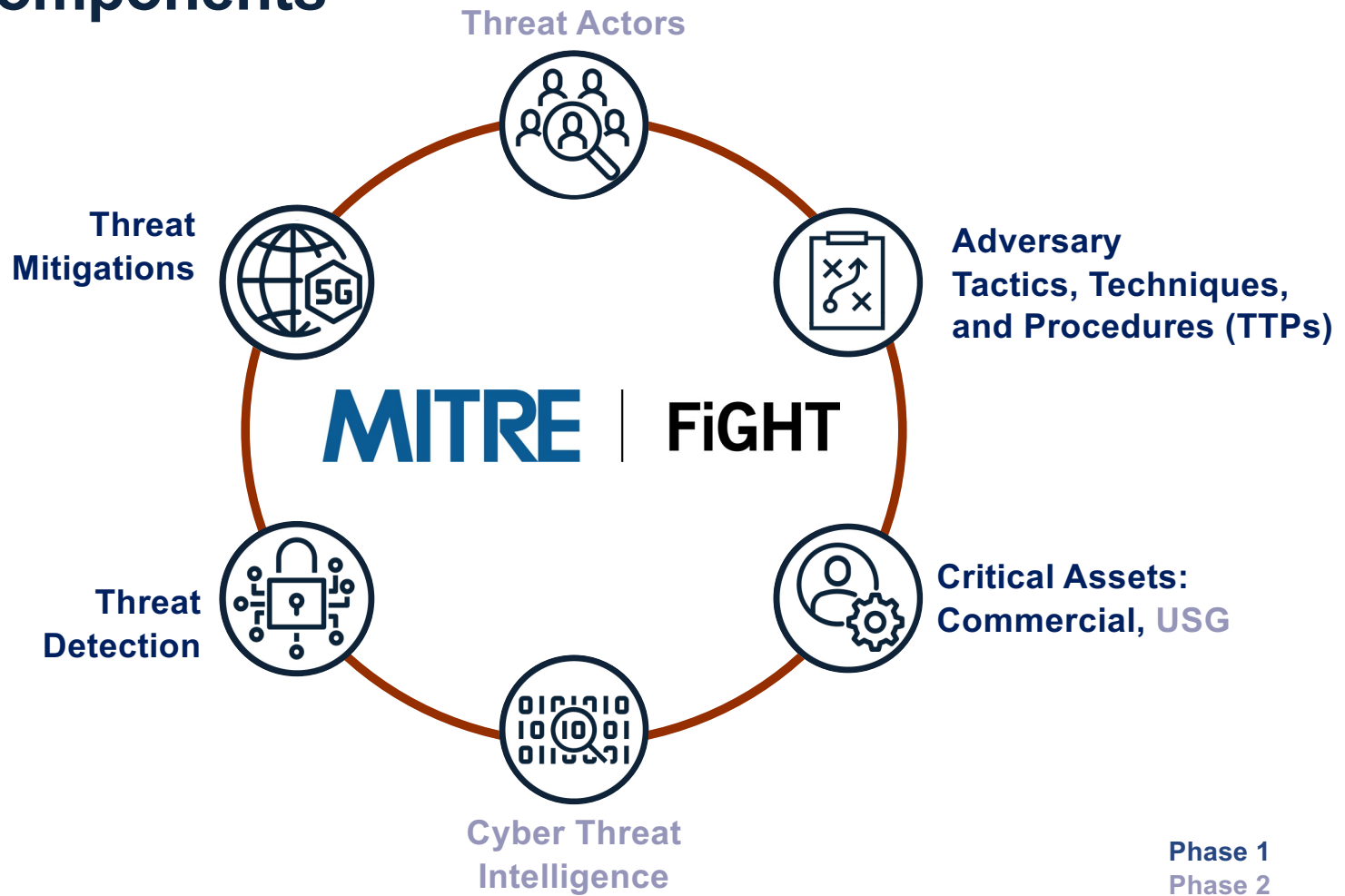


Acquisition planning



Security automation

FiGHT™ Components



FiGHT™ Philosophy

- **A threat model that documents adversary behaviors relevant to 5G**
- **Leverages concepts from ATT&CK but is a separate framework**
- **Sources:**
 - Empirical Observation - adversary behaviors from contributed threat intel.
 - Proof of Concept - adversary behaviors successfully demonstrated in a laboratory setting
 - Predictive - conceptual adversary behaviors not yet demonstrated in a laboratory setting or in the wild
- **Fitting behaviors into a threat model is iterative journey/subject to discussion**

Highly Abstract
Lockheed Martin Kill Chain,
Microsoft STRIDE

Mid-tier Abstraction
ATT&CK and FiGHT

Detailed
MITRE CVE, CWE, CAPEC

FiGHT™ Matrix

Launched Sept. 2022

<https://fight.mitre.org>

MITRE FiGHT™ v1.0.0															
Matrix Data Sources Mitigations Tactics Techniques Resources															
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact	Fraud	
1 technique	2 techniques	8 techniques	3 techniques	4 techniques	2 techniques	9 techniques	5 techniques	14 techniques	4 techniques	17 techniques	1 technique	2 techniques	10 techniques	6 techniques	
Gather Victim Host Information	Acquire Infrastructure Stage Capabilities	Software Deployment Tools Exploit Public-Facing Application Supply Chain Compromise DNS Manipulation Unauthorized access to Network Exposure Function (NEF) via token fraud Exploit Semi-public Facing Application Valid Accounts Trusted Relationship	Software Deployment Tools Registration of malicious network functions gNodeB Component Manipulation	Implant Internal Image DNS Manipulation Valid Accounts Pre-OS Boot	Escape to Host Valid Accounts	Rootkit Network Boundary Bridging Bypass home routing Weaken Integrity Spoof network slice identifier Valid Accounts Pre-OS Boot Impair Defenses Weaken Encryption	Network Sniffing Supply Chain Compromise Credentials from Password Stores Adversary-in-the-Middle Container Administration Command Valid Accounts Pre-OS Boot Impair Defenses Weaken Encryption	Remote System Discovery Remote Services Network Sniffing Network Service Scanning Network Function Service Discovery Network Flow Manipulation Locate UE Malicious VNF Instantiation Shared resource discovery Call Detail Record (CDR) collection Identify UE Discover network slice identifier Automated Exfiltration Container Administration Command	Remote Services Software Deployment Tools Escape to Host Unauthorized access to Network Exposure Function (NEF) via token fraud	Network Sniffing Exploit Public-Facing Application Eavesdrop on Insecure Network Communication Network-side SMS collection Network Flow Manipulation Memory Scraping Redirection of traffic via user plane network function Fraudulent AMF registration for UE in UDM Locate UE Malicious VNF Instantiation Abuse of Inter-operator Interfaces Call Detail Record (CDR) collection Identify UE Retrieve UE subscription data Spoof network slice identifier Exploit Semi-public Facing Application Adversary-in-the-	Standard Application Layer Protocol Automated Exfiltration	Exfiltration Over Alternative Protocol Automated Exfiltration	Exploit Public-Facing Application Jamming or Denial of Service Endpoint Denial of Service Redirection of traffic via user plane network function Device Database Manipulation Vandalism of Network Infrastructure Tunnel Endpoint ID (TEID) uniqueness failure Data Manipulation Trusted Relationship Network Denial of Service	Abuse of Inter-operator Interfaces Alter Subscriber Profile Charging fraud via NF control SIM boxing Falsify interconnect invoice SIM cloning	



MITRE FiGHT™ and MITRE ATT&CK® are a trademark and registered trademark of The MITRE Corporation. Approved for Public Release; Distribution Unlimited. Public Release Case Number 22-2192 @2022 The MITRE Corporation. ALL RIGHTS RESERVED.

CONTACT US

©2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PUBLIC RELEASE CASE NUMBER 23-1945

FiGHT™ can be operationalized

See The Threat

Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 14 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques
Replication Through Removable Media	Native API	BITS Jobs	Process Injection (8,71)	Obfuscated Files or Information (5,5)	Credentials from Password Stores (3,7)	System Information Discovery	Replication Through Removable Media	Screen Capture
Drive-by-Compromise	Windows Management Instrumentation	Hijack Execution Flow (7,11)	Traffic Signaling (2,1)	Deobfuscate/Decode Files or Information	Network Sniffing	File and Directory Discovery	Lateral Tool Transfer	Data from Local System
Valid Accounts (2,4)	Command and Scripting Interpreter (7,8)	Valid Accounts (2,4)	Exploitation for Privilege Escalation	Modify Registry	OS Credential Dumping (4,8)	Process Discovery	Archive Collected Data (3,3)	Audio Capture
Exploit Public-Facing Application	Exploitation for Client Execution	Account Manipulation (1,4)	Hijack Execution Flow (7,11)	Process Injection (8,1)	Brute Force (3,4)	System Network Configuration Discovery	Remote Services	Clipboard Data
External Remote Services	Scheduled Task/Job (3,8)	Browser Extensions	Valid Accounts (2,4)	Indicator Removal on Host (3,8)	Steal Web Session Cookie	System Owner/User Discovery	Remote Services (4,8)	Video Capture
Hardware Additions	Software Deployment Tools	Boot or Logon Automation (4,12)	Boot or Logon Automation (4,12)	Access Token Manipulation (6,9)	Two-Factor Authentication Interception	Query Registry	Remote Services (4,8)	Automated Collection
Phishing (2,7)	Internal Process Communication (2,2)	Compromised Client Software	Group Policy Modification	Virtualization/Sandbox Evasion (3,3)	Unsecured Credentials (4,8)	System Time Discovery	Remote Services (4,8)	Data from Removable Media
Supply Chain Compromise (1,3)	System Services (2,7)	External Remote Services	Scheduled Task/Job (3,8)	BITS Jobs	Exploitation for Credential Access	System Service Discovery	Internal Spearphishing	Man in the Browser
Trusted Relationship	User Execution (2,7)	Abuse Elevation Control Mechanism (4,4)	Hijack Execution Flow (7,11)	Abuse Elevation Control Mechanism (4,4)	Forced Authentication	Peripheral Device Discovery	Remote Service Session Hijacking (3,7)	Data from Network Shared Drive
		Scheduled Task/Job (3,8)	Boot or Logon Initialization Scripts (3,8)	Traffic Signaling (2,1)	Input Capture (3,4)	Remote System Discovery	Use Alternate Authentication Material (2,4)	Data from Cloud Storage Object
		External Remote Services	Create or Modify System	Group Policy	Application Window Discovery			Data from Configuration Repository (3,7)

Emulate Adversaries

Initial Access	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration
Features	Accessibility Features	Binary Padding	Brute Force	Account Discovery	Application Deployment Software	Command-Line	Automated Collection	Automated Exfiltration
Output System	Appinit DLLs	Bypass User Account Control	Credential Dumping	Application Window Discovery	Exploitation of Vulnerability	Execution through API	Clipboard Data	Data Compressed
	By-pass User Account Control	Code Signing	Credential Manipulation	File and Directory Discovery	Logon Scripts	Graphical User Interface	Data Staged	Data Encrypted
	DLL Injection	Component Firmware	Credentials in Files	Local Network Configuration Discovery	Pass the Hash	PowerShell	Data from Local System	Transfer Size Limits
Host File	DLL Search Order Hijacking	DLL Injection	Exploitation of Vulnerability	Local Network Connection Discovery	Pass the Ticket	Process Hollowing	Data from Network Shared Drive	Exfiltration Over Alternative Protocol
Firmware	Exploitation of Vulnerability	DLL Search Order Hijacking	Input Capture	Network Service Scanning	Remote Desktop Protocol	Rundll32	Data from Removable Media	Exfiltration Over Command and Control Channel
Order Hijacking	Legitimate Credentials	Disc Side-Loading	Network Sniffing	Peripheral Device Discovery	Remote File Copy	Scheduled Task	Email Collection	Exfiltration Over Other Network Medium
	Local Port Monitor	Disabling Security Tools	Two-Factor Authentication Interception	Permission Groups Discovery	Remote Services	Service Execution	Input Capture	Exfiltration Over Physical Medium
Credentials	New Service	Exploitation of Vulnerability	Process Discovery	Replication Through Removable Media	Third-party Software	Screen Capture	Scheduled Transfer	

Develop Analytics

```
#Parse log file for failed login attempts
failed_attempts=$(grep "authentication failure"
/var/log/auth.log)
# Write failed attempts to log file
if [ -n "$failed_attempts" ]; then
echo "$failed_attempts" >> "$log_file"
fi
```

Assess Your Defenses

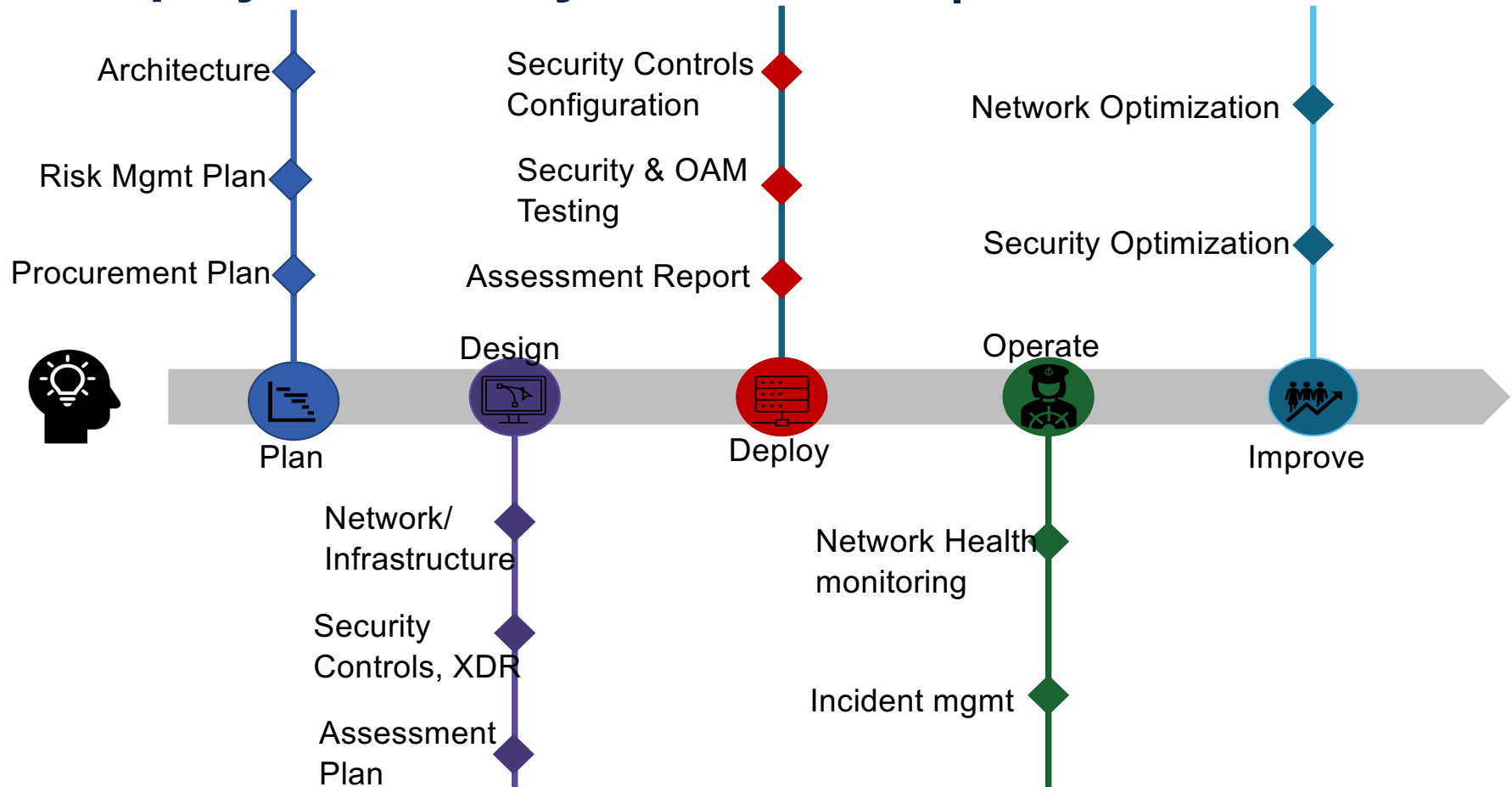
Category	Sub-category	Confidence of Detection
Initial Access	Valid Accounts	High Confidence of Detection
Initial Access	Exploit Public-Facing Application	Some Confidence of Detection
Initial Access	Phishing	Low Confidence of Detection
Initial Access	Supply Chain Compromise	High Confidence of Detection
Initial Access	Trusted Relationship	Some Confidence of Detection
Execution	Command and Scripting Interpreter	High Confidence of Detection
Execution	Exploitation for Client Execution	Some Confidence of Detection
Execution	External Remote Services	High Confidence of Detection
Execution	Internal Process Communication	Some Confidence of Detection
Execution	System Services	High Confidence of Detection
Execution	User Execution	Some Confidence of Detection
Persistence	BITS Jobs	High Confidence of Detection
Persistence	Hijack Execution Flow	Some Confidence of Detection
Persistence	Valid Accounts	High Confidence of Detection
Persistence	Browser Extensions	Some Confidence of Detection
Persistence	Boot or Logon Automation	High Confidence of Detection
Persistence	Compromised Client Software	Some Confidence of Detection
Persistence	External Remote Services	High Confidence of Detection
Persistence	Abuse Elevation Control Mechanism	Some Confidence of Detection
Persistence	Scheduled Task/Job	High Confidence of Detection
Persistence	System Services	Some Confidence of Detection
Persistence	User Execution	High Confidence of Detection
Privilege Escalation	Process Injection	High Confidence of Detection
Privilege Escalation	Exploitation for Privilege Escalation	Some Confidence of Detection
Privilege Escalation	Hijack Execution Flow	High Confidence of Detection
Privilege Escalation	Valid Accounts	Some Confidence of Detection
Privilege Escalation	Boot or Logon Automation	High Confidence of Detection
Privilege Escalation	Group Policy Modification	Some Confidence of Detection
Privilege Escalation	Scheduled Task/Job	High Confidence of Detection
Privilege Escalation	Abuse Elevation Control Mechanism	Some Confidence of Detection
Privilege Escalation	External Remote Services	High Confidence of Detection
Privilege Escalation	System Services	Some Confidence of Detection
Privilege Escalation	User Execution	High Confidence of Detection
Defense Evasion	Obfuscated Files or Information	High Confidence of Detection
Defense Evasion	Deobfuscate/Decode Files or Information	Some Confidence of Detection
Defense Evasion	Modify Registry	High Confidence of Detection
Defense Evasion	Process Injection	Some Confidence of Detection
Defense Evasion	Rootkit	High Confidence of Detection
Defense Evasion	Indicator Removal on Host	Some Confidence of Detection
Defense Evasion	Access Token Manipulation	High Confidence of Detection
Defense Evasion	Virtualization/Sandbox Evasion	Some Confidence of Detection
Defense Evasion	Group Policy	High Confidence of Detection
Defense Evasion	System Time Discovery	Some Confidence of Detection
Defense Evasion	System Service Discovery	High Confidence of Detection
Defense Evasion	Peripheral Device Discovery	Some Confidence of Detection
Defense Evasion	Remote System Discovery	High Confidence of Detection
Defense Evasion	Use Alternate Authentication Material	Some Confidence of Detection
Defense Evasion	Application Window Discovery	High Confidence of Detection
Credential Access	Credentials from Password Stores	High Confidence of Detection
Credential Access	Network Sniffing	Some Confidence of Detection
Credential Access	OS Credential Dumping	High Confidence of Detection
Credential Access	Brute Force	Some Confidence of Detection
Credential Access	Steal Web Session Cookie	High Confidence of Detection
Credential Access	Two-Factor Authentication Interception	Some Confidence of Detection
Credential Access	Unsecured Credentials	High Confidence of Detection
Credential Access	Exploitation for Credential Access	Some Confidence of Detection
Credential Access	Forced Authentication	High Confidence of Detection
Credential Access	Internal Spearphishing	Some Confidence of Detection
Credential Access	Remote Service Session Hijacking	High Confidence of Detection
Credential Access	Use Alternate Authentication Material	Some Confidence of Detection
Credential Access	Application Window Discovery	High Confidence of Detection
Discovery	System Information Discovery	High Confidence of Detection
Discovery	File and Directory Discovery	Some Confidence of Detection
Discovery	Process Discovery	High Confidence of Detection
Discovery	System Network Configuration Discovery	Some Confidence of Detection
Discovery	System Owner/User Discovery	High Confidence of Detection
Discovery	Query Registry	Some Confidence of Detection
Discovery	System Network Connections Discovery	High Confidence of Detection
Discovery	System Time Discovery	Some Confidence of Detection
Discovery	System Service Discovery	High Confidence of Detection
Discovery	Peripheral Device Discovery	Some Confidence of Detection
Discovery	Remote System Discovery	High Confidence of Detection
Discovery	Use Alternate Authentication Material	Some Confidence of Detection
Discovery	Application Window Discovery	High Confidence of Detection
Lateral Movement	Lateral Tool Transfer	High Confidence of Detection
Lateral Movement	Archive Collected Data	Some Confidence of Detection
Lateral Movement	Remote Services	High Confidence of Detection
Lateral Movement	Taint Shared Content	Some Confidence of Detection
Lateral Movement	Automated Collection	High Confidence of Detection
Lateral Movement	Data from Removable Media	Some Confidence of Detection
Lateral Movement	Internal Spearphishing	High Confidence of Detection
Lateral Movement	Man in the Browser	Some Confidence of Detection
Lateral Movement	Remote Service Session Hijacking	High Confidence of Detection
Lateral Movement	Data from Network Shared Drive	Some Confidence of Detection
Lateral Movement	Data from Cloud Storage Object	High Confidence of Detection
Lateral Movement	Data from Configuration Repository	Some Confidence of Detection
Lateral Movement	Screen Capture	High Confidence of Detection
Lateral Movement	Clipboard Data	Some Confidence of Detection
Lateral Movement	Data Staged	High Confidence of Detection
Lateral Movement	Data Encrypted	Some Confidence of Detection
Lateral Movement	Data from Local System	High Confidence of Detection
Lateral Movement	Transfer Size Limits	Some Confidence of Detection
Lateral Movement	Exfiltration Over Alternative Protocol	High Confidence of Detection
Lateral Movement	Exfiltration Over Command and Control Channel	Some Confidence of Detection
Lateral Movement	Exfiltration Over Other Network Medium	High Confidence of Detection
Lateral Movement	Exfiltration Over Physical Medium	Some Confidence of Detection
Lateral Movement	Scheduled Transfer	High Confidence of Detection

Legend
High Confidence of Detection
Some Confidence of Detection
Low Confidence of Detection

FiGHT™ can be used to perform threat-informed defense in risk management and operations.

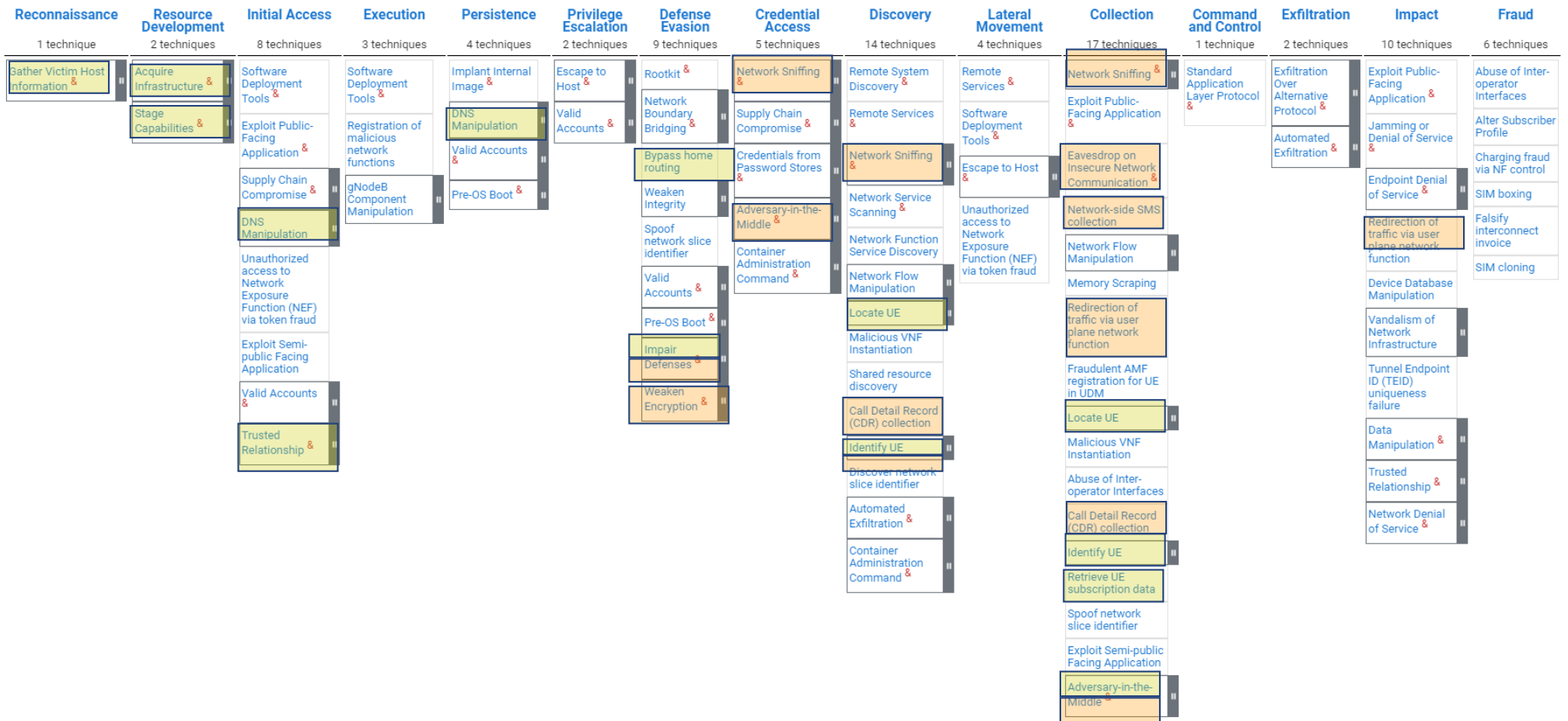


5G Deployment life cycle: FiGHT™ | ATT&CK® informed



Threats relevant to **untrusted commercial deployments**

Adversary Goal 1: identify and locate UE; Goal 2: intercept UE communications



Threats relevant tactical deployments

Adversary goal: intercept or disrupt communications

Example

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact	Fraud
1 technique	2 techniques	8 techniques	3 techniques	4 techniques	2 techniques	9 techniques	5 techniques	14 techniques	4 techniques	17 techniques	1 technique	2 techniques	10 techniques	6 techniques
Gather Victim Host Information &	Acquire Infrastructure & Stage Capabilities &	Software Deployment Tools & Exploit Public-Facing Application & Supply Chain Compromise & DNS Manipulation & Unauthorized access to Network Exposure Function (NEF) via token fraud & Exploit Semi-public Facing Application & Valid Accounts & Trusted Relationship &	Software Deployment Tools & Registration of malicious network functions & gNodeB Component Manipulation &	Implant Internal Image & DNS Manipulation & Valid Accounts & Pre-OS Boot &	Escape to Host & Valid Accounts &	Rootkit & Network Boundary Bridging & Bypass home routing & Weaken Integrity & Spoof network slice identifier & Valid Accounts & Pre-OS Boot & Impair Defenses & Weaken Encryption &	Network Sniffing & Supply Chain Compromise & Credentials from Password Stores & Adversary-in-the-Middle & Container Administration Command &	Remote System Discovery & Remote Services & Network Sniffing & Network Service Scanning & Network Function Service Discovery & Network Flow Manipulation & Locate UE & Malicious VNF Instantiation & Shared resource discovery & Call Detail Record (CDR) collection & Identify UE & Discover network slice identifier & Automated Exfiltration & Container Administration Command &	Remote Services & Software Deployment Tools & Escape to Host & Unauthorized access to Network Exposure Function (NEF) via token fraud &	Network Sniffing & Exploit Public-Facing Application & Eavesdrop on Insecure Network Communication & Network-side SMS collection & Network Flow Manipulation & Memory Scraping & Redirection of traffic via user plane network function & Fraudulent AMF registration for UE in UDM & Locate UE & Malicious VNF Instantiation & Abuse of Inter-operator Interfaces & Call Detail Record (CDR) collection & Identify UE & Retrieve UE subscription data & Spoof network slice identifier & Exploit Semi-public Facing Application & Adversary-in-the-Middle &	Standard Application Layer Protocol & Exfiltration Over Alternative Protocol & Automated Exfiltration &	Exploit Public-Facing Application & Jamming or Denial of Service & Endpoint Denial of Service & Redirection of traffic via user plane network function & Device Database Manipulation & Vandalism of Network Infrastructure & Tunnel Endpoint ID (TEID) uniqueness failure & Data Manipulation & Trusted Relationship & Network Denial of Service &	Abuse of Inter-operator Interfaces & Alter Subscriber Profile & Charging fraud via NF control & SIM boxing & Falsify interconnect invoice & SIM cloning &	

FiGHT Tooling

Tools	Tool Use	Status
FiGHT Pipeline	Creation and editing of the threat model	90% complete
FiGHT Navigator	Visual application of the threat model for scenarios building	80% complete
STIX & TAXII	Intelligence sharing STIX – model TAXII – communication method	70% complete Not started
FiGHT Workbench	User-side editing of the threat model	Not started
FiGHT Flow	Visual modeling of adversary emulation over time	Not started
CALDERA	Automated adversary emulation for red team assessment	Not started

FiGHT summary - DOD

Ensure that the DOD can design, deploy and manage secure tactical networks, and operate through commercial 5G networks whenever and wherever

Achievements:

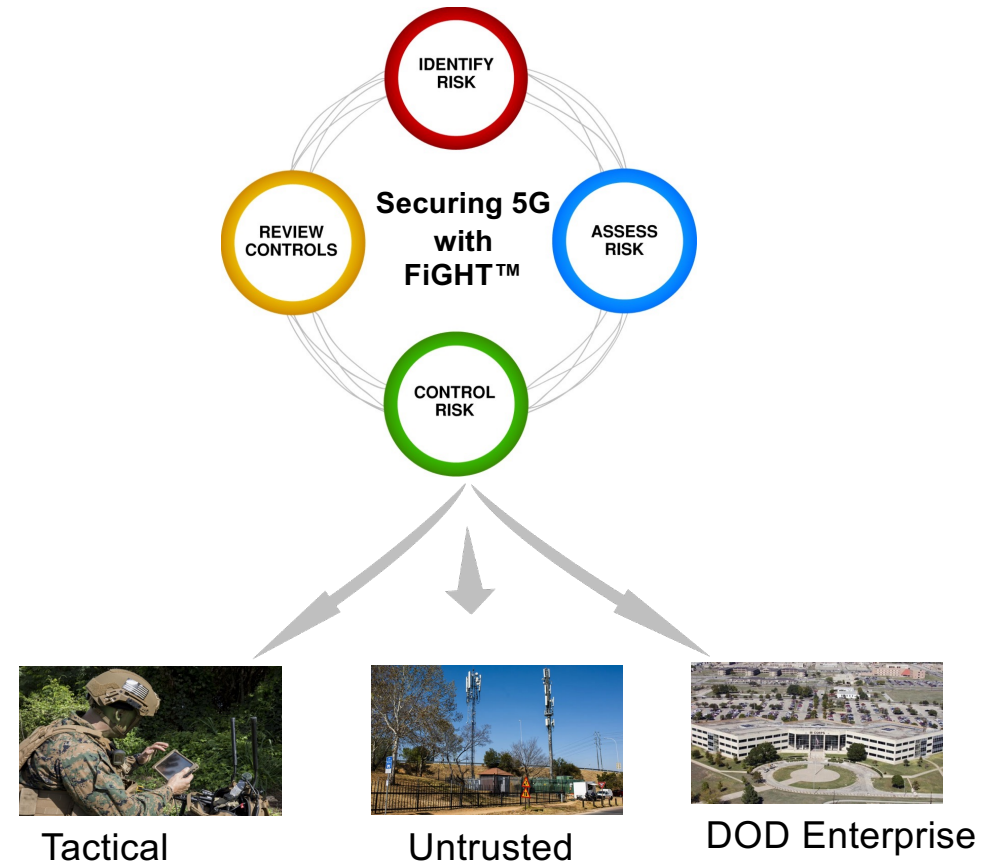
- Developed and published threat-based framework <https://fight.mitre.org>
- Continually modernize/extend capability
- Collaborate with vendors, community (e.g., GSMA)

Goals:

- Lab testing of techniques
- Support/collaborate with government sponsors and operators

Impact:

- Enables to operationalize security hardening detection and mitigation techniques --- to protect DOD assets and communication from adversary activity



MITRE | **FiGHT**

fight@mitre.org

<https://fight.mitre.org>

MITRE | SOLVING PROBLEMS
FOR A SAFER WORLD™