LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

LLNL-TR-858139

Requirements and Recommendations for a Physical Attack Characterization Framework

J. K. McGrath, H. R. Scott, L. R. Slone

December 7, 2023

Disclaimer

This document was prepared as an account of work sponsored by an agency of the United States government. Neither the United States government nor Lawrence Livermore National Security, LLC, nor any of their employees makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States government or Lawrence Livermore National Security, LLC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC, and shall not be used for advertising or product endorsement purposes.

This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.

LLNL-TR-858139

Lawrence Livermore
National Laboratory

Requirements and Recommendations for a Physical Attack Characterization Framework

Jenna McGrath, Ph.D.
Heather Scott
Llewelyn Slone

Lawrence Livermore National Laboratory

Unclassified

July 2023

Technical Report Prepared for:
Infrastructure Security Division (ISD), Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS)

Disclaimer

This document was prepared as an account of work sponsored by an agency of the United States government. Neither the United States government nor Lawrence Livermore National Security, LLC, nor any of their employees makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States government or Lawrence Livermore National Security, LLC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC, and shall not be used for advertising or product endorsement purposes.

Lawrence Livermore National Laboratory is operated by Lawrence Livermore National Security, LLC, for the U.S. Department of Energy, National Nuclear Security Administration under Contract DE-AC52-07NA27344.

Table of Contents

Table of Tables

Table of Figures

1 Introduction and Summary

1.1 Project Motivation and Overview

This study seeks to identify existing frameworks or develop requirements and recommendations for a new framework that can consistently characterize physical attacks, analogous to MITRE ATT&CK®. MITRE ATT&CK is widely used across government, research organizations, and the cyber security community to characterize cyber attack tactics, techniques, and procedures (TTPs) in a consistent and commonly understood manner. While physical attack taxonomies, methodologies, and other tools for evaluating physical security do exist, many are sector and/or facility-type specific—and therefore not able to provide comparable scenarios across sectors—or are more focused on security assessment instead of the characterization of attacks themselves. A MITRE ATT&CK analog for physical attacks on critical infrastructure would provide a common language and structure for analysis of physical attacks.

Cyber and Physical Security Convergence is formal collaboration between previously disjointed cybersecurity and physical security functions within an organization.

Source: Cybersecurity and Infrastructure Security Agency

Existing attack characterization methodologies do not robustly address cyber-physical security risks. To fully understand a facility's security needs, it is important to understand the entire vulnerability landscape from both a physical and a cyber perspective. To underscore this need, organizations such as the Cybersecurity and Infrastructure Security Agency (CISA) are calling for a coordinated approach to cyber and physical security, which they refer to as cyber and physical security convergence.[1] A physical attack characterization framework that could be used jointly with MITRE ATT&CK would help support a more robust analysis in support of convergence, enabling the consistent characterization of attacks that utilize both cyber and physical tactics and techniques. This could provide analysts and stakeholders with a clearer understanding of how security mitigations deployed in the physical realm impact security risks in the cyber realm, and vice versa.

In this study, the project team evaluates existing physical security taxonomies and methodologies to assess whether an existing method can be used to create a "physical half" of MITRE ATT&CK. This study then provides requirements and recommendations for a framework that can leverage aspects of existing methodologies. The goal of the final framework is for it to be widely adopted and referenced, regardless of critical infrastructure sector, facility type, or facility components. This study also identifies applicable use cases for when and how a framework could be applied across the various critical infrastructure sectors for a variety of attack types or motivations.

Through a literature review of existing security-focused methodologies and taxonomies, engagement with relative stakeholders, evaluation of potential physical attack framework use

[1] "Cybersecurity and Physical Security Convergence," *CISA*, December 22, 2021, 1–4, https://www.cisa.gov/sites/default/files/publications/Cybersecurity%2520and%2520Physical%2520Security%2520Convergence_508_01.05.2021.pdf.

cases, and subsequent identification of requirements, this study identified the following key findings and recommendations:

- There is a need for a new physical attack characterization framework.
- A physical attack framework should be interoperable with the MITRE ATT&CK framework.
- A physical attack framework should be broadly applicable, but with detailed tactics, techniques, and procedures that encompass the entire attack path.
- A physical attack framework should be based on observed or feasible events.
- A physical attack framework should adapt features from existing methodologies, frameworks, and taxonomies.
- A physical attack framework should be owned, overseen, and maintained by one organization.

1.2 Cyber and Physical Security Convergence: Definitions

The growth of computers and computer systems in the assets and processes that comprise and protect critical infrastructure has been accompanied by a growing attack surface for adversaries. While adversaries once had to use solely physical means, they may now choose from a wide range of both cyber and physical actions with which to plan, prepare for, and execute an attack. This diversity creates new combined cyber-physical attack paths that critical infrastructure stakeholders must understand and defend against. While MITRE ATT&CK provides an industry-standard method for characterizing cyber-only attack paths, a physical counterpart is currently lacking. Before we examine the requirements for a physical attack framework, however, it is useful to define several terms.

To begin, we borrow the concept of an "attack path," as defined in the *DHS Risk Lexicon*, and examine its attributes.

- ***Attack Path:*** Steps that an adversary takes or may take to plan, prepare for, and execute an attack (DHS Risk Lexicon).[2] An attack path is comprised of cyber actions, physical actions, or both.
    - Lockheed Martin's Cyber Kill Chain® is an example of the attack path concept applied to cyber defense.[3]
- ***Endpoint Action:*** The individual attack path step that directly causes harm to the target (typically characterized by the weapon and delivery method).[4]
- ***Combined Cyber-Physical Attack Path:*** Attack path that includes both physical and cyber actions.

[2] "DHS Risk Lexicon" (Department of Homeland Security - Risk Steering Committee, September 2010), https://www.cisa.gov/resources-tools/resources/dhs-risk-lexicon.

[3] "Lockheed Martin Cyber Kill Chain®," accessed August 8, 2023, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

[4] Partially derived from the definition for "attack method" as found in the *DHS Risk Lexicon*: "Manner and means, including the weapon and delivery method, an adversary may use to cause harm on a target." See "DHS Risk Lexicon."

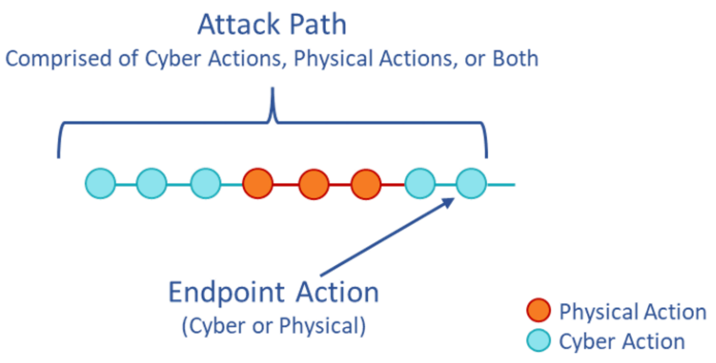


Figure 1. Attack Path and Endpoint Action

As Figure 1 shows, the attack path is comprised of actions, which can be entirely physical, entirely cyber, or a mix of both. The action that directly causes harm to the target is the endpoint action. As described below, attack types are defined by the domain of their endpoint actions—either cyber or physical.

- ***Physical Attack:*** Actions taken by an adversary to cause harm to a target using a physical endpoint action. (The attack path can be physical-only or combined cyber-physical).
- ***Cyber Attack:*** Actions taken by an adversary to cause harm to a target using a cyber endpoint action. (The attack path can be cyber-only or combined cyber-physical).

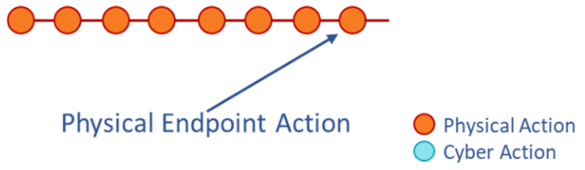


Figure 2. Physical Attack

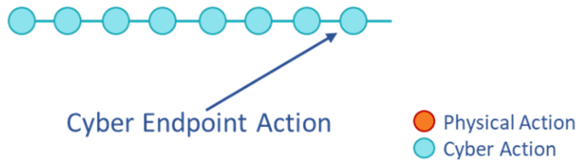


Figure 3. Cyber Attack

As shown in Figure 2 and Figure 3, an attack with a physical endpoint action is a "physical attack" and an attack with a cyber endpoint action is a "cyber attack."[5]

[5] Note, the definitions for these terms begin by specifying that the actions are taken by an "adversary," defined in the *DHS Risk Lexicon* as an "individual, group, organization, or government that conducts or has the intent to conduct detrimental activities." While this presupposes a malign intent, for clarity, the definitions reiterate the actions are carried out "to cause harm."

As noted in the definitions, although the name of the attack is dictated by its endpoint action, the attack path may include a mix of actions from either domain. For example, a cyber attack which aims to deploy malware on a system may involve a physical break-in to insert a removable media drive into a computer. Conversely, a physical attack which aims to physically destroy a particular component may involve a cyber intrusion to acquire codes that allow access to the building. Specific definitions for attacks with mixed paths are provided below.

- ***Cyber-Enabled Physical Attack***: A physical attack that includes one or more cyber actions in its attack path (the attack path is inherently combined). See Figure 4.
- ***Physical-Enabled Cyber Attack***: A cyber attack that includes one or more physical actions in its attack path (the attack path is inherently combined). See Figure 5.

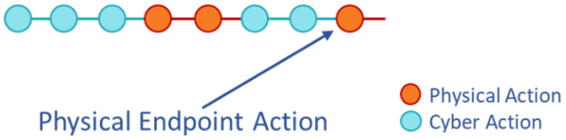


Figure 4. Cyber-Enabled Physical Attack

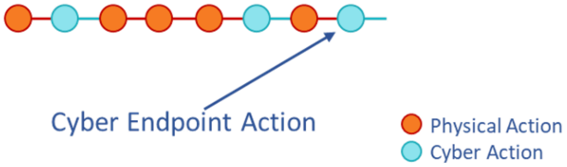


Figure 5. Physical-Enabled Cyber Attack

While these definitions clarify the meaning of an attack path and several types of attacks, they do not specify the adversary's options for each step along the attack path (i.e. the specific tactics, techniques, and procedures).[6] MITRE ATTK&CK provides this for cyber-only attack paths, but without a physical attack framework, analysts and security personnel are left without a consistent source of TTPs for physical-only or—crucially for goals related to cyber and physical security convergence—combined cyber-physical attack paths. This study aims to provide the requirements and recommendations for such a framework.

[6] "Tactics, techniques, and procedures" are defined by NIST as "the behavior of an actor. A tactic is the highest-level description of this behavior, while techniques give a more detailed description of behavior in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique." See "Tactics, Techniques, and Procedures (TTP)," NIST Information Technology Laboratory Computer Security Resource Center, accessed August 8, 2023, https://csrc.nist.gov/glossary/term/tactics_techniques_and_procedures.

2 Review of Existing Physical Security Methodologies and Taxonomies

This section summarizes existing methodologies and taxonomies that are primarily used to analyze physical security risks. Several methodologies addressing cyber security and information security are also included as they provide potentially useful elements for developers of a physical attack framework.

The research conducted in this part of the study consisted of open-source research into physical security evaluation processes, attack characterization methodologies, and other applicable frameworks. The project team also conducted interviews with stakeholders associated with various critical infrastructure sectors, government agencies, research organizations, and groups within Lawrence Livermore National Laboratory (LLNL) involved in security analysis. The review took care to include methods used across a variety of sectors and for different purposes, but it is not an exhaustive list of all relevant processes the physical security community may use. An overview of each method is presented in the remainder of this section.

2.1 MITRE ATT&CK

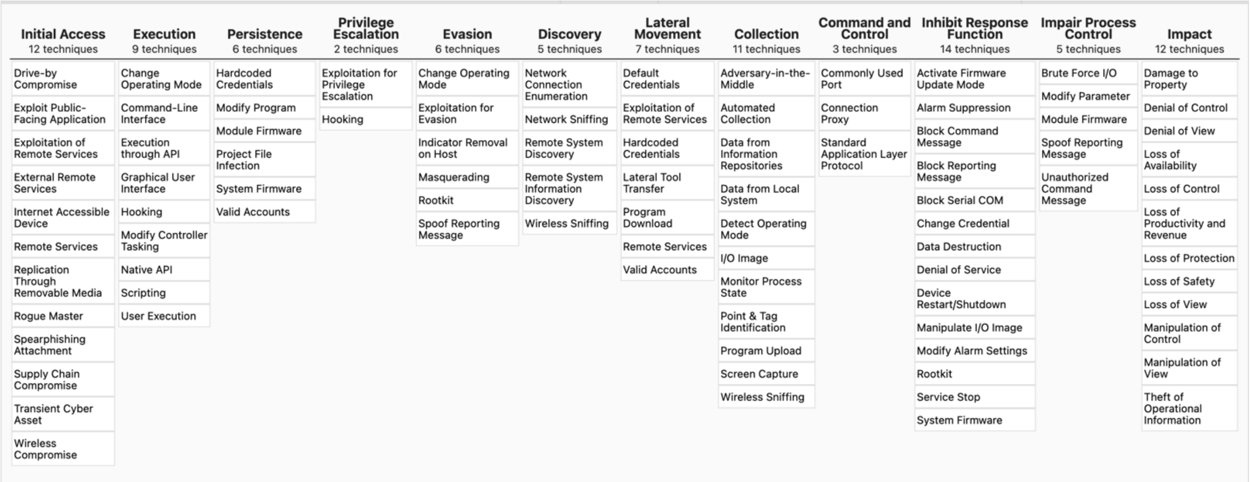
MITRE ATT&CK was developed in 2013 by the not-for-profit MITRE Corporation to categorize adversarial tactics, techniques, and common knowledge (ATT&CK) in an accessible matrix structure. The purpose of MITRE ATT&CK is to present a knowledge base of adversary tactics and techniques based on real-world observations and is used as a foundation for the development of specific threat models and methodologies across multiple sectors.[7] MITRE has three ATT&CK matrices for different types of systems: Enterprise, Mobile, and Industrial Control Systems (ICS). The three matrices include a combination of TTPs that are unique to each system along with TTPs that apply to multiple systems. The Enterprise matrix shows TTPs unique to specific operating systems, networks, cloud providers, and platforms.[8] The Mobile matrix offers unique TTPs for Android or Apple iOS mobile operating systems.[9] The ICS matrix, shown in Figure 6, outlines TTPs unique to industrial control systems.[10]

[7] "MITRE ATT&CK®," accessed July 28, 2023, https://attack.mitre.org/.

[8] "Matrix - Enterprise | MITRE ATT&CK®," accessed July 28, 2023, https://attack.mitre.org/matrices/enterprise/.

[9] "Matrix - Mobile | MITRE ATT&CK®," accessed July 28, 2023, https://attack.mitre.org/matrices/mobile/.

[10] "Matrix ICS | MITRE ATT&CK®," accessed July 28, 2023, https://attack.mitre.org/matrices/ics/.



Initial Access 12 techniques	Execution 9 techniques	Persistence 6 techniques	Privilege Escalation 2 techniques	Evasion 6 techniques	Discovery 5 techniques	Lateral Movement 7 techniques	Collection 11 techniques	Command and Control 3 techniques	Inhibit Response Function 14 techniques	Impair Process Control 5 techniques	Impact 12 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Replication Through Removable Media	Native API					Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Rogue Master	Scripting						Point & Tag Identification		Denial of Service		Loss of Safety
Spearphishing Attachment	User Execution						Program Upload		Device Restart/Shutdown		Loss of View
Supply Chain Compromise							Screen Capture		Manipulate I/O Image		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
Wireless Compromise									Rootkit		Theft of Operational Information
									Service Stop		
									System Firmware		

Figure 6. MITRE ATT&CK Matrix for ICS[11]

Each matrix is organized around a set of adversary tactics, which follow an attack path structure, ranging from early steps such as reconnaissance or initial access through impact. MITRE ATT&CK does not require the tactics to occur in a set order (or occur at all).[12] Within each tactic, MITRE includes techniques, sub-techniques, procedure examples, mitigations, and other useful information.[13] The ATT&CK TTPs are detailed enough for users to understand and apply, but are not so detailed that a user would be constrained in applying them to a variety of use cases.[14]

Updates to the ATT&CK matrices are based on either observed or feasible incidents. Specifically, MITRE uses publicly available threat intelligence, incident reporting, and publicly available research on new techniques that closely align with common adversary actions.[15]

While MITRE ATT&CK is used across many critical infrastructure sectors, it is only applicable to cyber attacks (i.e. attacks with cyber endpoints) and generally only includes cyber actions. There are several tactics that include a physical action (such as gaining initial access through exploitation of removable media); however, these are rare within ATT&CK. Aside from these few instances, MITRE ATT&CK does not consider combined cyber-physical attack paths and its ability to support analysis of cyber and physical security convergence as a stand-alone framework is limited.

2.2 Design Basis Threat (DBT)

According to the Nuclear Regulatory Commission (NRC), a Design Basis Threat (DBT) is "a description of the type, composition, and capabilities of an adversary, against which a security system is designed to protect."[16] The NRC uses DBT "as a basis for designing safeguards systems

[11] "Matrix ICS | MITRE ATT&CK®."

[12] Blake E. Strom et al., "MITRE ATT&CK®: Design and Philosophy" (McLean, VA: MITRE, March 2020), 4–13, https://www.mitre.org/sites/default/files/2021-11/prs-19-01075-28-mitre-attack-design-and-philosophy.pdf.

[13] "MITRE ATT&CK®," accessed July 18, 2023, https://attack.mitre.org/.

[14] Blake E. Strom, "ATT&CK 101," *MITRE.Org*, May 3, 2018, https://medium.com/mitre-attack/att-ck-101-17074d3bc62.

[15] "FAQ | MITRE ATT&CK®," accessed July 28, 2023, https://attack.mitre.org/resources/faq/.

[16] "Design-Basis Threat (DBT)," NRC Web, February 15, 2023, https://www.nrc.gov/reading-rm/basic-ref/glossary/design-basis-threat-dbt.html.

to protect against acts of radiological sabotage and to prevent the theft of special nuclear material."[17]

Though primarily used by the nuclear security community, DBT has seen widespread adoption across many types of facilities. During the project team's stakeholder interviews, nearly every government organization and group within LLNL identified DBT as a starting point for physical security assessment in their specific area.[18] Though not a physical attack characterization methodology, the DBT process is easily adaptable and customizable and many physical security professionals recommended it as a useful way to consider physical threats across sectors and agnostic of facility type.[19]

2.3 Army Tactics, Techniques, and Procedures (No. 3-39.32): Physical Security

Army Tactics, Techniques, and Procedures: Physical Security (ATTP 3-39.32) provides a training reference for personnel who are responsible for planning and executing U.S. military physical security programs.[20] ATTP 3-39.32 is intended to be used along with other Department of Defense (DoD) and Army publications, including the Security Engineering Unified Facilities Criteria (discussed below).[21]

ATTP 3-39.32 contains eleven chapters concerning physical security, including topics such as: physical security challenges; the use of site- and facility-specific physical security planning committees; the importance of coordinated policies, plans, and procedures during the physical security planning process; and adversary tactics and techniques.[22] The guide also covers security aspects to consider during site design, including mitigation efforts to increase physical security of a site (such as barriers, lighting, electronic security systems, access control points, locking mechanisms, and on-site security personnel). [23]

2.4 United Facilities Criteria: DoD Minimum Antiterrorism Standards for Buildings

The intent of the of the Unified Facilities Criteria (UFC): DoD Minimum Antiterrorism Standards for Buildings is to "establish minimum engineering standards that incorporate antiterrorism (AT) based mitigation measures" in order to "reduce collateral damage and the scope and severity of mass casualties in the event of a terrorist attack."[24] The standards were created in partial response to the 1996 truck bombing of the United States Air Force 4404 Provisional Wing at the Khobar

[17] "Design-Basis Threat (DBT)."

[18] Based on interviews with LLNL stakeholders conducted during March through April 2023.

[19] Based on interviews with LLNL stakeholders conducted during March through April 2023.

[20] "Physical Security," Army Tactics, Techniques, and Procedures, August 2010, https://irp.fas.org/doddir/army/attp3-39-32.pdf.

[21] "Physical Security," v.

[22] "Physical Security."

[23] "Physical Security," v-vi.

[24] "Unified Facilities Criteria (UFC) - DoD Minimum Antiterrorism Standards For Buildings," UFC, December 12, 2018, 1, https://www.wbdg.org/FFC/DOD/UFC/ufc_4_010_01_2018_c2.pdf.

Towers in Saudi Arabia.[25] After the bombing, the committee to investigate found that were no standards for force protection in fixed DoD facilities.[26]

The standards are mandatory and apply to new constructions, existing DoD inhabited buildings, and inhabited tenant buildings on DoD installations, including DoD expeditionary structures, with limited exceptions.[27] The UFC standards provide a set of minimum engineering standards for all sites, regardless of whether a facility requires additional specific protection standards based on the location or purpose of the facility.[28]

The UFC standards assume a variety of terrorist tactics ranging from external explosive threats to mail bombs to chemical, biological, and radiological weapons.[29] They include standards for a wide array of facility components, including items as diverse as trash containers, revolving doors, and heating and cooling systems.[30] They also include representative standoff distances for a variety of walls, roofs, and windows commonly used in DoD construction (see Figure 7 for an example).[31] While the information in the UFC standards is specifically designed for a DoD audience, the breadth of weapons and mitigations it includes could provide useful inputs to developers of a physical attack framework.

[25] Bruce Reidel, "Remembering the Khobar Towers Bombing," *Brookings*, June 21, 2021, https://www.brookings.edu/articles/remembering-the-khobar-towers-bombing/.

[26]

"Unified Facilities Criteria (UFC) - DoD Minimum Antiterrorism Standards For Buildings," 1.

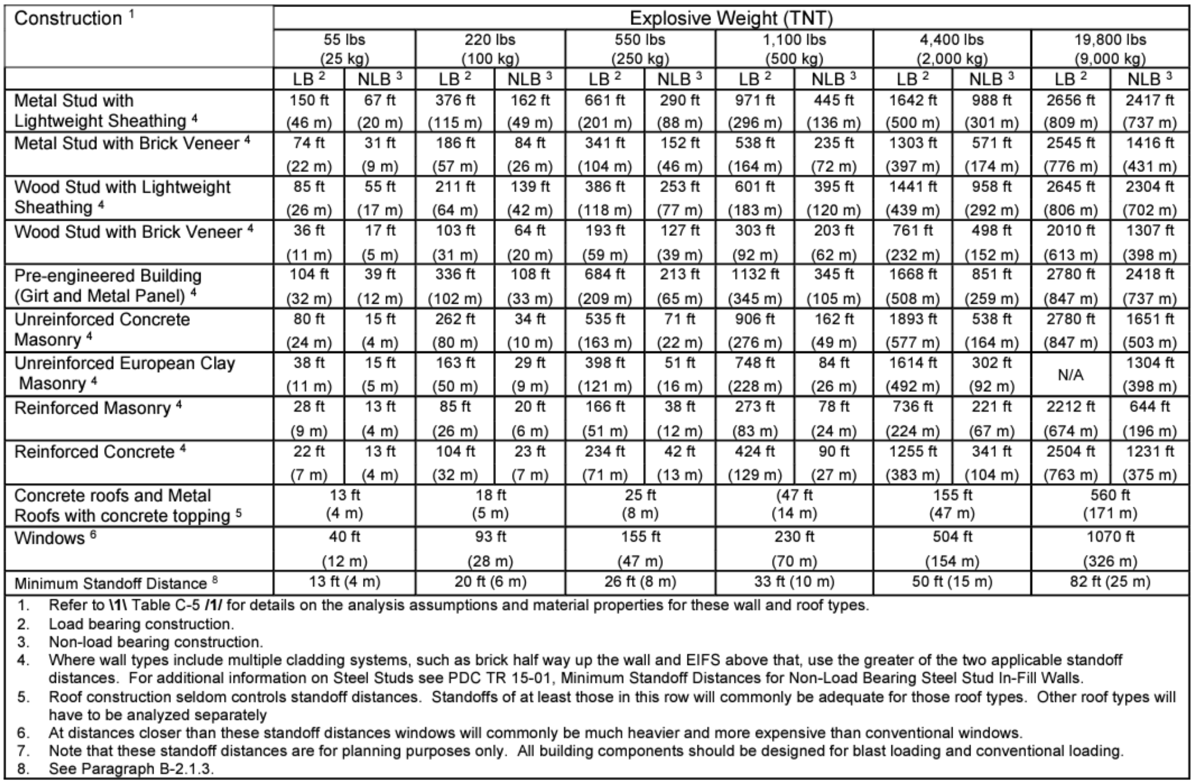
[27] "Unified Facilities Criteria (UFC) - DoD Minimum Antiterrorism Standards for Buildings," 2.

[28] "Unified Facilities Criteria (UFC) - DoD Minimum Antiterrorism Standards for Buildings," 7.

[29] "Unified Facilities Criteria (UFC) - DoD Minimum Antiterrorism Standards for Buildings," 15.

[30] "Unified Facilities Criteria (UFC) - DoD Minimum Antiterrorism Standards for Buildings," 17–35.

[31] "Unified Facilities Criteria (UFC) - DoD Minimum Antiterrorism Standards for Buildings," 59–67.



Construction [1]	Explosive Weight (TNT)											
	55 lbs (25 kg)		220 lbs (100 kg)		550 lbs (250 kg)		1,100 lbs (500 kg)		4,400 lbs (2,000 kg)		19,800 lbs (9,000 kg)	
	LB [2]	NLB [3]	LB [2]	NLB [3]	LB [2]	NLB [3]	LB [2]	NLB [3]	LB [2]	NLB [3]	LB [2]	NLB [3]
Metal Stud with Lightweight Sheathing [4]	150 ft (46 m)	67 ft (20 m)	376 ft (115 m)	162 ft (49 m)	661 ft (201 m)	290 ft (88 m)	971 ft (296 m)	445 ft (136 m)	1642 ft (500 m)	988 ft (301 m)	2656 ft (809 m)	2417 ft (737 m)
Metal Stud with Brick Veneer [4]	74 ft (22 m)	31 ft (9 m)	186 ft (57 m)	84 ft (26 m)	341 ft (104 m)	152 ft (46 m)	538 ft (164 m)	235 ft (72 m)	1303 ft (397 m)	571 ft (174 m)	2545 ft (776 m)	1416 ft (431 m)
Wood Stud with Lightweight Sheathing [4]	85 ft (26 m)	55 ft (17 m)	211 ft (64 m)	139 ft (42 m)	386 ft (118 m)	253 ft (77 m)	601 ft (183 m)	395 ft (120 m)	1441 ft (439 m)	958 ft (292 m)	2645 ft (806 m)	2304 ft (702 m)
Wood Stud with Brick Veneer [4]	36 ft (11 m)	17 ft (5 m)	103 ft (31 m)	64 ft (20 m)	193 ft (59 m)	127 ft (39 m)	303 ft (92 m)	203 ft (62 m)	761 ft (232 m)	498 ft (152 m)	2010 ft (613 m)	1307 ft (398 m)
Pre-engineered Building (Girt and Metal Panel) [4]	104 ft (32 m)	39 ft (12 m)	336 ft (102 m)	108 ft (33 m)	684 ft (209 m)	213 ft (65 m)	1132 ft (345 m)	345 ft (105 m)	1668 ft (508 m)	851 ft (259 m)	2780 ft (847 m)	2418 ft (737 m)
Unreinforced Concrete Masonry [4]	80 ft (24 m)	15 ft (4 m)	262 ft (80 m)	34 ft (10 m)	535 ft (163 m)	71 ft (22 m)	906 ft (276 m)	162 ft (49 m)	1893 ft (577 m)	538 ft (164 m)	2780 ft (847 m)	1651 ft (503 m)
Unreinforced European Clay Masonry [4]	38 ft (11 m)	15 ft (5 m)	163 ft (50 m)	29 ft (9 m)	398 ft (121 m)	51 ft (16 m)	748 ft (228 m)	84 ft (26 m)	1614 ft (492 m)	302 ft (92 m)	N/A	1304 ft (398 m)
Reinforced Masonry [4]	28 ft (9 m)	13 ft (4 m)	85 ft (26 m)	20 ft (6 m)	166 ft (51 m)	38 ft (12 m)	273 ft (83 m)	78 ft (24 m)	736 ft (224 m)	221 ft (67 m)	2212 ft (674 m)	644 ft (196 m)
Reinforced Concrete [4]	22 ft (7 m)	13 ft (4 m)	104 ft (32 m)	23 ft (7 m)	234 ft (71 m)	42 ft (13 m)	424 ft (129 m)	90 ft (27 m)	1255 ft (383 m)	341 ft (104 m)	2504 ft (763 m)	1231 ft (375 m)
Concrete roofs and Metal Roofs with concrete topping [5]	13 ft (4 m)		18 ft (5 m)		25 ft (8 m)		(47 ft (14 m)		155 ft (47 m)		560 ft (171 m)	
Windows [6]	40 ft (12 m)		93 ft (28 m)		155 ft (47 m)		230 ft (70 m)		504 ft (154 m)		1070 ft (326 m)	
Minimum Standoff Distance [8]	13 ft (4 m)		20 ft (6 m)		26 ft (8 m)		33 ft (10 m)		50 ft (15 m)		82 ft (25 m)	

1. Refer to **\1** Table C-5 **/1/** for details on the analysis assumptions and material properties for these wall and roof types.
2. Load bearing construction.
3. Non-load bearing construction.
4. Where wall types include multiple cladding systems, such as brick half way up the wall and EIFS above that, use the greater of the two applicable standoff distances. For additional information on Steel Studs see PDC TR 15-01, Minimum Standoff Distances for Non-Load Bearing Steel Stud In-Fill Walls.
5. Roof construction seldom controls standoff distances. Standoffs of at least those in this row will commonly be adequate for those roof types. Other roof types will have to be analyzed separately
6. At distances closer than these standoff distances windows will commonly be much heavier and more expensive than conventional windows.
7. Note that these standoff distances are for planning purposes only. All building components should be designed for blast loading and conventional loading.
8. See Paragraph B-2.1.3.

Figure 7. UFC DoD Minimum Antiterrorism Standards for Buildings: Representative Standoff Distances for Very Low-Level Building Construction Protection[32]

2.5 Criticality, Accessibility, Recuperability, Vulnerability, Effect and Recognizability (CARVER) Matrix

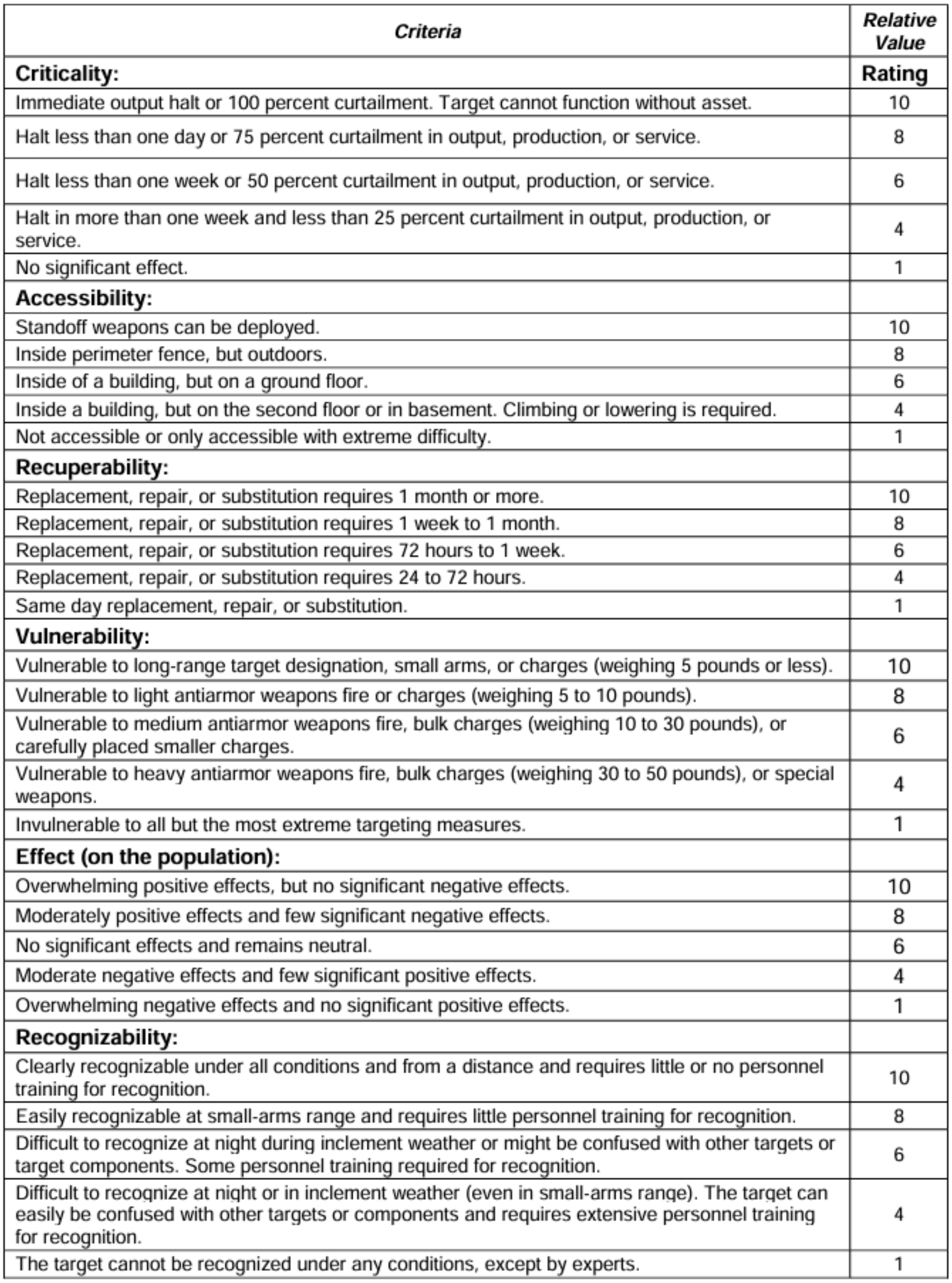
The CARVER matrix was developed by U.S. Special Forces to assess enemy infrastructure for potential targeting. The matrix includes the following target selection criteria: criticality, accessibility, recuperability, vulnerability, effect, and recognizability.[33] For targeting purposes, the matrix is used from the enemy or aggressor's perspective to assess the hardness or softness of targets[34] (i.e. target selection) and criticality to the mission's success.[35] CARVER can also be used jointly with the MSHARPP matrix, discussed below.

[32] "Unified Facilities Criteria (UFC) - DoD Minimum Antiterrorism Standards for Buildings," 61.

[33] Christopher M. Schnaubelt, Eric V. Larson, and Matthew E. Boyer, *Vulnerability Assessment Method Pocket Guide: A Tool for Center of Gravity Analysis* (Santa Monica, CA: RAND Arroyo Center, 2014), 29–32, https://www.rand.org/content/dam/rand/pubs/tools/TL100/TL129/RAND_TL129.pdf.

[34] "Police Intelligence Operations," Army Tactics, Techniques, and Procedures, No. 3-39.20 (FM 3-19.50), July 2010, 5–18, https://irp.fas.org/doddir/army/fm3-19-50.pdf.

[35] "Protection," Army Doctrine Reference Publication, No. 3-37 (FM 3-37), August 2012, 2–6, https://irp.fas.org/doddir/army/adrp3_37.pdf.



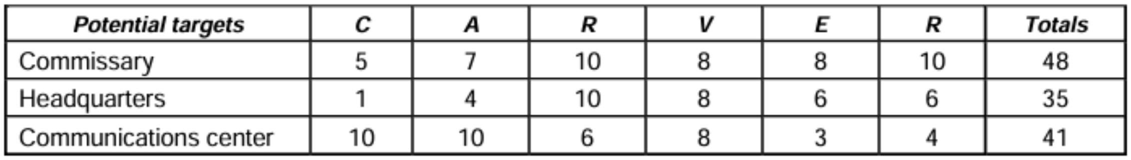
Criteria	*Relative Value*
Criticality:	**Rating**
Immediate output halt or 100 percent curtailment. Target cannot function without asset.	10
Halt less than one day or 75 percent curtailment in output, production, or service.	8
Halt less than one week or 50 percent curtailment in output, production, or service.	6
Halt in more than one week and less than 25 percent curtailment in output, production, or service.	4
No significant effect.	1
Accessibility:	
Standoff weapons can be deployed.	10
Inside perimeter fence, but outdoors.	8
Inside of a building, but on a ground floor.	6
Inside a building, but on the second floor or in basement. Climbing or lowering is required.	4
Not accessible or only accessible with extreme difficulty.	1
Recuperability:	
Replacement, repair, or substitution requires 1 month or more.	10
Replacement, repair, or substitution requires 1 week to 1 month.	8
Replacement, repair, or substitution requires 72 hours to 1 week.	6
Replacement, repair, or substitution requires 24 to 72 hours.	4
Same day replacement, repair, or substitution.	1
Vulnerability:	
Vulnerable to long-range target designation, small arms, or charges (weighing 5 pounds or less).	10
Vulnerable to light antiarmor weapons fire or charges (weighing 5 to 10 pounds).	8
Vulnerable to medium antiarmor weapons fire, bulk charges (weighing 10 to 30 pounds), or carefully placed smaller charges.	6
Vulnerable to heavy antiarmor weapons fire, bulk charges (weighing 30 to 50 pounds), or special weapons.	4
Invulnerable to all but the most extreme targeting measures.	1
Effect (on the population):	
Overwhelming positive effects, but no significant negative effects.	10
Moderately positive effects and few significant negative effects.	8
No significant effects and remains neutral.	6
Moderate negative effects and few significant positive effects.	4
Overwhelming negative effects and no significant positive effects.	1
Recognizability:	
Clearly recognizable under all conditions and from a distance and requires little or no personnel training for recognition.	10
Easily recognizable at small-arms range and requires little personnel training for recognition.	8
Difficult to recognize at night during inclement weather or might be confused with other targets or target components. Some personnel training required for recognition.	6
Difficult to recognize at night or in inclement weather (even in small-arms range). The target can easily be confused with other targets or components and requires extensive personnel training for recognition.	4
The target cannot be recognized under any conditions, except by experts.	1

Figure 8. Example CARVER Criteria Evaluation Tool[36]

Sample CARVER matrix scoring criteria are shown in Figure 8. While users can start at any point in the matrix to begin assessment, each of the six criteria need to be addressed for proper use of

[36] "Police Intelligence Operations," 5–19.

the tool. The details of each criteria and the relative scores can be adjusted depending on the use case but must remain consistent throughout the entire assessment.[37] An example of the final scoring output is shown in Figure 9, in which the highest total values represent the most valuable targets.



Potential targets	***C***	***A***	***R***	***V***	***E***	***R***	***Totals***
Commissary	5	7	10	8	8	10	48
Headquarters	1	4	10	8	6	6	35
Communications center	10	10	6	8	3	4	41

Figure 9. Example CARVER Matrix[38]

2.6 Mission, Symbolism, History, Accessibility, Recognizability, Proximity, Population (MSHARPP) Matrix

Like CARVER, the MSHARPP matrix is also a DoD vulnerability and criticality assessment tool. The matrix includes the following criteria: mission, symbolism, history, accessibility, recognizability, proximity, and population.[39] Unlike CARVER, MSHARPP assess the value of potential targets "from the inside out"—i.e. from the perspective of the owner or user.[40] MSHARPP is designed to assess personnel vulnerabilities, but it can also be used for broader analysis focused on facilities or other assets.[41]

Users can customize the assessment of the seven criteria in the matrix to meet the needs of the facility or site being assessed. The MSHARPP matrix results in a score that represents the value of the target—with higher scores representing higher value.[42] Figure 10 provides a sample MSHARPP scoring matrix output.

From an infrastructure protection perspective, the MSHARPP and CARVER matrices can be used together to assess the value of a potential target (i.e. a facility or other asset) from two points of view—i.e. the value the infrastructure has for the user and the value of the asset as a target for an attacker.[43]

[37] Schnaubelt, Larson, and Boyer, *Vulnerability Assessment Method Pocket Guide*, 29–31.

[38] "Police Intelligence Operations," 5–20.

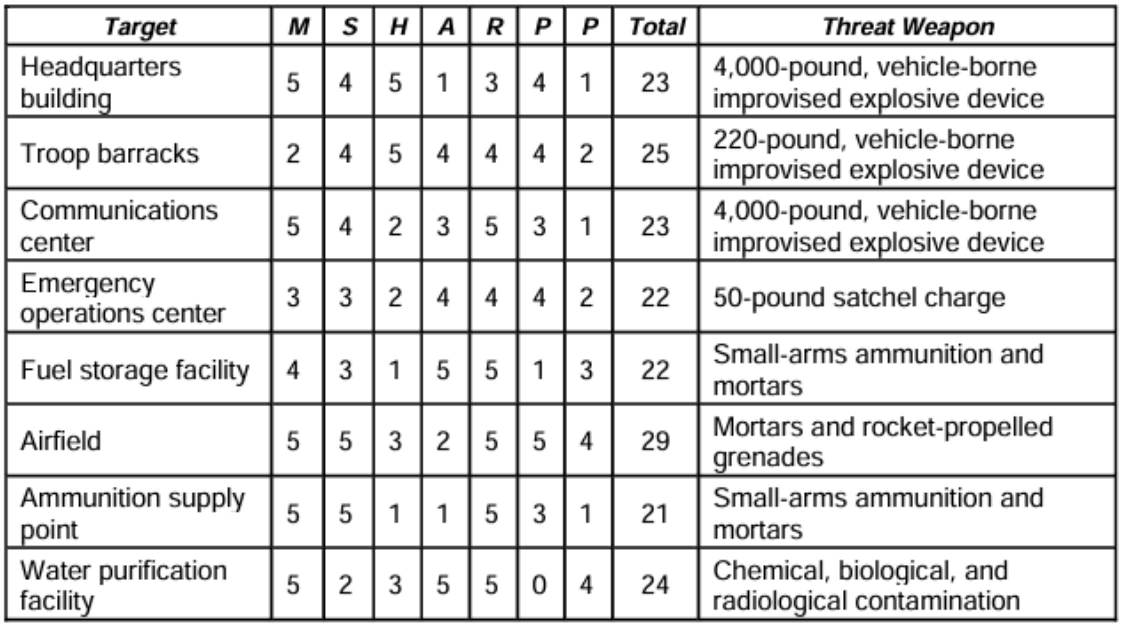
[39] "Police Intelligence Operations," 5–18.

[40] Schnaubelt, Larson, and Boyer, *Vulnerability Assessment Method Pocket Guide*, 107.

[41] "Police Intelligence Operations," 5–18.

[42] António Ferreira, "Vulnerability Analysis in Critical Infrastructures: A Methodology," *Security and Defense Quarterly* 24, no. 2 (June 28, 2019): 65–86, https://doi.org/10.35467/sdq/108665.

[43] Ferreira, 65–86.



Target	*M*	*S*	*H*	*A*	*R*	*P*	*P*	*Total*	*Threat Weapon*
Headquarters building	5	4	5	1	3	4	1	23	4,000-pound, vehicle-borne improvised explosive device
Troop barracks	2	4	5	4	4	4	2	25	220-pound, vehicle-borne improvised explosive device
Communications center	5	4	2	3	5	3	1	23	4,000-pound, vehicle-borne improvised explosive device
Emergency operations center	3	3	2	4	4	4	2	22	50-pound satchel charge
Fuel storage facility	4	3	1	5	5	1	3	22	Small-arms ammunition and mortars
Airfield	5	5	3	2	5	5	4	29	Mortars and rocket-propelled grenades
Ammunition supply point	5	5	1	1	5	3	1	21	Small-arms ammunition and mortars
Water purification facility	5	2	3	5	5	0	4	24	Chemical, biological, and radiological contamination

Figure 10. Sample MSHARPP Matrix[44]

2.7 Infrastructure Security Tool (IST)

The Infrastructure Security Tool (IST) is used by CISA across all critical infrastructure sectors to assess a facility's security and resiliency. The IST focuses on:

- Identifying facilities' physical security, security forces, security management, information sharing, protective measures, and dependencies related to preparedness, mitigation, response, resilience, and recovery.
- Identifying security areas of possible improvements.
- Creating facility protective and resilience measures indices that show a comparison to similar facilities that have completed ISTs.
- Tracking progress toward improving critical infrastructure security.[45]

A facility's owners/operators voluntarily request assessment and work with a CISA security advisor to complete a site visit and survey.[46] CISA provides the assessment information to the owners/operators via both a written report and a secure, interactive, web-based user dashboard. The dashboard displays scores across a variety of factors and allows the facility's staff to see how their facility compares to its peers (e.g. a hospital is compared to other hospitals, or a K-12 school is compared to other K-12 schools) via the Protective Measures Index (PMI) and Resilience Measures Index (RMI) (see below for additional details). Facility representatives can then work

[44] "Police Intelligence Operations," 5–18.

[45] "Infrastructure Survey Tool Fact Sheet" (CISA, n.d.), https://www.cisa.gov/sites/default/files/2023-02/cisa20ist20fact20sheet.pdf.

[46] Anthony J. Masys, ed., "US Department of Homeland Security (DHS) Vulnerability Assessment Application Examples," in *Handbook of Security Science* (Cham, Switzerland: Springer Nature, 2022), 12, https://books.google.com/books?id=hdCPEAAAQBAJ&lpg=PA3&ots=vf8Tp73rSf&dq=cisa%20infrastructure%20security%20tool%20ist&lr&pg=PA12#v=onepage&q=cisa%20infrastructure%20security%20tool%20ist&f=false.

within the dashboard to understand how the implementation of certain mitigation strategies could improve their scores. Some mitigation strategies may work better at certain facilities—e.g. additional perimeter fencing around a water treatment plant may help deter intruders or disrupt line of sight into the facility, but perimeter fencing around hospitals may inadvertently and unnecessarily limit access. Details gathered about different facility types, applicable mitigation strategies, potential variability across populations or locations, and potential vulnerabilities are available in the written report and the IST Dashboard.[47]

The IST benefits from having both a physical-focused and a cyber-focused questionnaire. However, the two forms cannot be merged at this time, and each require distinct types of expertise by the security advisor. While the IST is a detailed assessment and analysis tool, ultimately it is focused on characterizing a facility's security profile and is not specifically designed to characterize attacks themselves.

2.8 Protective Measures Index (PMI) and Resilience Measures Index (RMI)

The information collected from the IST for an individual facility is used to calculate a Protective Measures Index (PMI) and a Resilience Measures Index (RMI). The PMI and RMI aim to capture the fundamental aspects of protection and resilience for critical infrastructure across all hazards.[48] The main objective of the PMI is to "measure the ability of a critical infrastructure system to resist to [sic] disruptive events" while the main objective of the RMI is to "measure the ability of a critical infrastructure to reduce the magnitude and/or duration of impacts from disruptive events."[49]

Both the PMI and RMI include multiple levels of components.[50] The major (Level 1) components of each are show in Figure 11 and

Figure 12 below. Level 2 and 3 subcomponents of the PMI are showing in Figure 13.

[47] "Infrastructure Survey Tool Fact Sheet."

[48] F.D. Petit et al., *Protective Measures Index and Vulnerability Index: Indicators of Critical Infrastructure Protection and Vulnerability*, 2013, vii, https://publications.anl.gov/anlpubs/2013/11/77931.pdf and F.D. Petit et al., *Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience* (Argonne National Laboratory, 2013), ix, https://publications.anl.gov/anlpubs/2013/07/76797.pdf.

[49] Petit et al., *Protective Measures Index and Vulnerability Index: Indicators of Critical Infrastructure Protection and Vulnerability*, vii and Petit et al., *Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience*, ix.

[50] Petit et al., *Protective Measures Index and Vulnerability Index: Indicators of Critical Infrastructure Protection and Vulnerability*, 10 and Petit et al., *Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience*, 9.

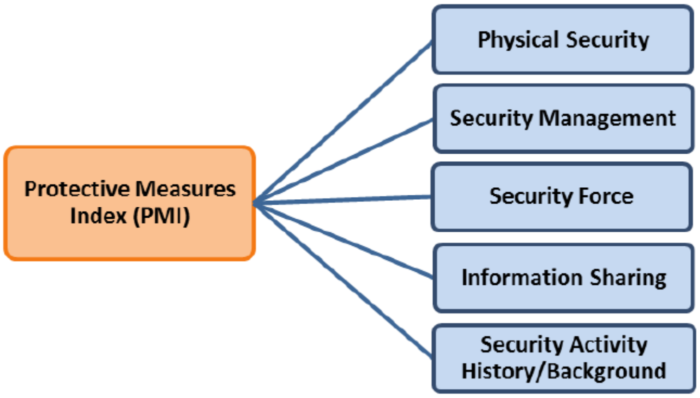


Figure 11. Level 1 Components of the PMI[51]

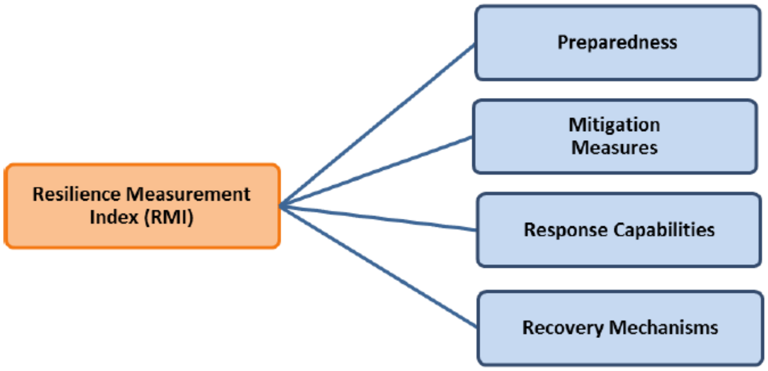


Figure 12. Level 1 Components of the PMI[52]

[51] Petit et al., *Protective Measures Index and Vulnerability Index: Indicators of Critical Infrastructure Protection and Vulnerability*, 10.

[52] Petit et al., *Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience*, 8.

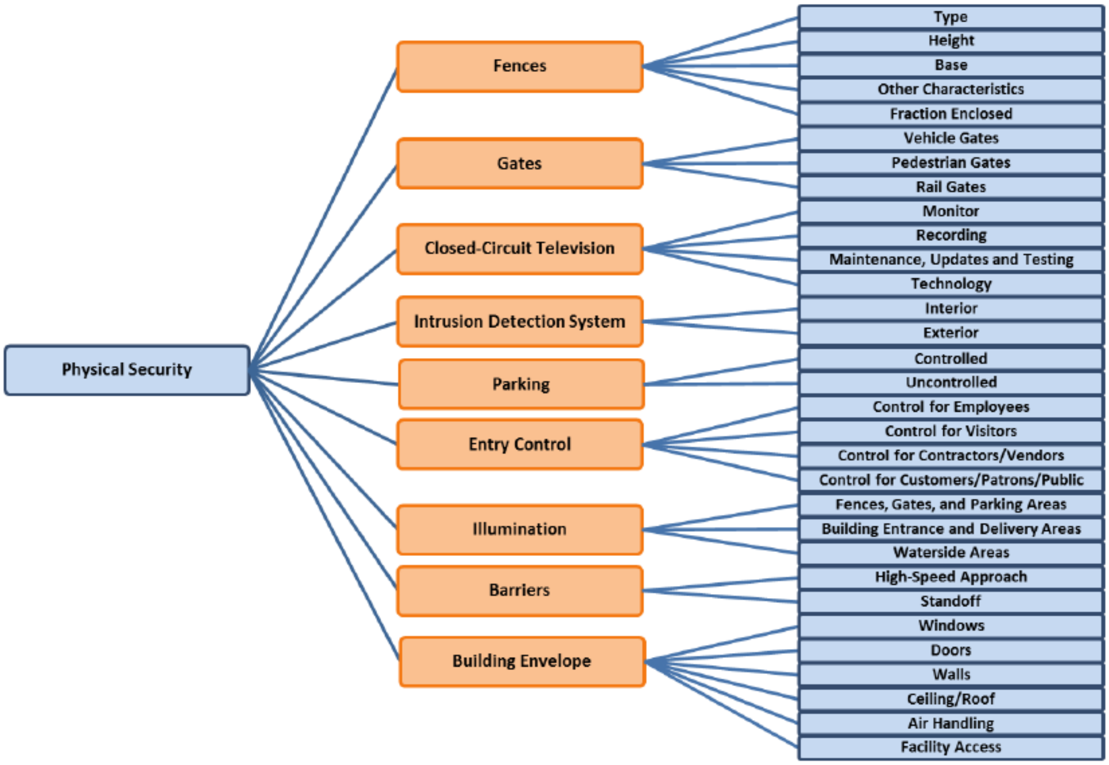


Figure 13. Levels 2 and 3 Subcomponents of the PMI Contributing to Physical Security[53]

Each component was weighted by subject matter experts to indicate its relative importance to a facility's protection or resilience. PMI and RMI values range between 0 (low protection/resilience) and 100 (high protection/resilience). PMI and RMI scores do not mean that a specific event will lead to a specific level of consequences for a given facility.[54] Instead, the PMI and RMI allow facilities to compare their levels of protection and resilience against those of other similar facilities and prioritize strategies for improving protection, lowering vulnerability, and improving resilience. The information also assists CISA in analyzing vulnerabilities in critical infrastructure sectors and subsectors so it can identify potential mitigations.[55]

The PMI and RMI provide robust lists of mitigation measures that contribute to protection and mitigation, which could be useful in the development of a physical attack framework. Ultimately, however, the two indexes focus on defensive measures and do not directly provide adversary tactics, techniques, or procedures.[56]

[53] Petit et al., *Protective Measures Index and Vulnerability Index: Indicators of Critical Infrastructure Protection and Vulnerability*, 11.

[54] Petit et al., vii and Petit et al., *Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience*, x.

[55] Petit et al., *Protective Measures Index and Vulnerability Index: Indicators of Critical Infrastructure Protection and Vulnerability*, vii and Petit et al., *Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience*, x.

[56] Petit et al., *Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience*, ix–x.

2.9 Security Assessment at First Entry (SAFE) Tool

The Security Assessment at First Entry (SAFE) tool is a streamlined variation of the IST. An assessment using the IST has multiple steps, an onsite visit, and a quality assurance evaluation process that requires a significant time commitment. The SAFE tool was developed to provide a quick security assessment for smaller-scale facilities, such as places of worship or small elections facilities.[57] As with the IST, SAFE is voluntary and hosted as a web application.[58]

The SAFE tool takes just a few hours to complete but uses similar language and a similar user interface design as the IST—making it easily adoptable by those already familiar with the IST. There are fewer questions in the SAFE assessment than the IST survey, with most focused on physical security and the remaining questions focused on planning, operations, and overall resiliency. The results of SAFE are emailed to the facility and, unlike the IST, there is not a web-based dashboard to allow comparison to other similar facilities.[59]

2.10 National Nuclear Security Administration (NNSA) Supplemental Directive 470.4-2: Enterprise Safeguards and Security Planning and Analysis Program

The purpose of NNSA Supplemental Directive 470.4-2: Enterprise Safeguards and Security Planning and Analysis Program (NNSA SD 470.4-2) is to provide "a consistent and standardized procedure for conducting a security risk assessment (SRA) or vulnerability assessment (VA) and reporting risk within the NNSA nuclear security enterprise" in order to create "a consistent set of deliverables to effect risk-informed decisions that result in an integrated, robust, effective, and efficient safeguards and security program."[60]

The NNSA SD 470.4-2 includes processes, methodologies, formats, and other information related to a variety of risk-management requirements, such as: modeling tools, asset characterization, target determination, analysis on sabotage of critical infrastructure or program assets, threat characterization, facility characterization, protective force characterization, scenario development, security plans, and others.[61] NNSA SD 470.4-2 also provides a responsibility matrix to clarify who is responsible for the development, review, and approval of safeguards and security risk-related documents.[62]

The applicability of NNSA SD 470.4-2 to physical attack characterization across all critical infrastructure sectors is limited by its focus on the nuclear security enterprise. The framework is complex, specific, and includes multiple layers of oversight for which other sectors or facilities may not have resources. However, its various components, such as standardized methods for analyzing sabotage, characterizing assets and facilities, and determining targets, may be helpful inputs in the development of a physical attack framework.

[57] "Security at First Entry Fact Sheet" (CISA, n.d.), https://www.cisa.gov/sites/default/files/2023-06/Security%20Assessment%20at%20First%20Entry%20%28SAFE%29%20Fact%20Sheet%202023.pdf and interviews with stakeholders conducted on May 16, 2023.

[58] "SAFE Fact Sheet."

[59] "SAFE Fact Sheet" and interviews with stakeholders conducted on May 16, 2023.

[60] "Enterprise Safeguards and Security Planning and Analysis Program," Supplemental Directive, NNSA SD 470.4-2 (National Nuclear Security Administration, June 23, 2018), 1, https://www.energy.gov/sites/prod/files/2018/07/f53/SD%20470.4-2%20ESSPAP.pdf.

[61] "Enterprise Safeguards and Security Planning and Analysis Program," 2–6.

[62] "Enterprise Safeguards and Security Planning and Analysis Program," AT2-1.

2.11 RAND Vulnerability Assessment Method (VAM)

RAND's VAM aims to "facilitate the identification or discovery of [information] system vulnerabilities" and "suggest relevant mitigation techniques."[63] VAM is implemented in six steps:

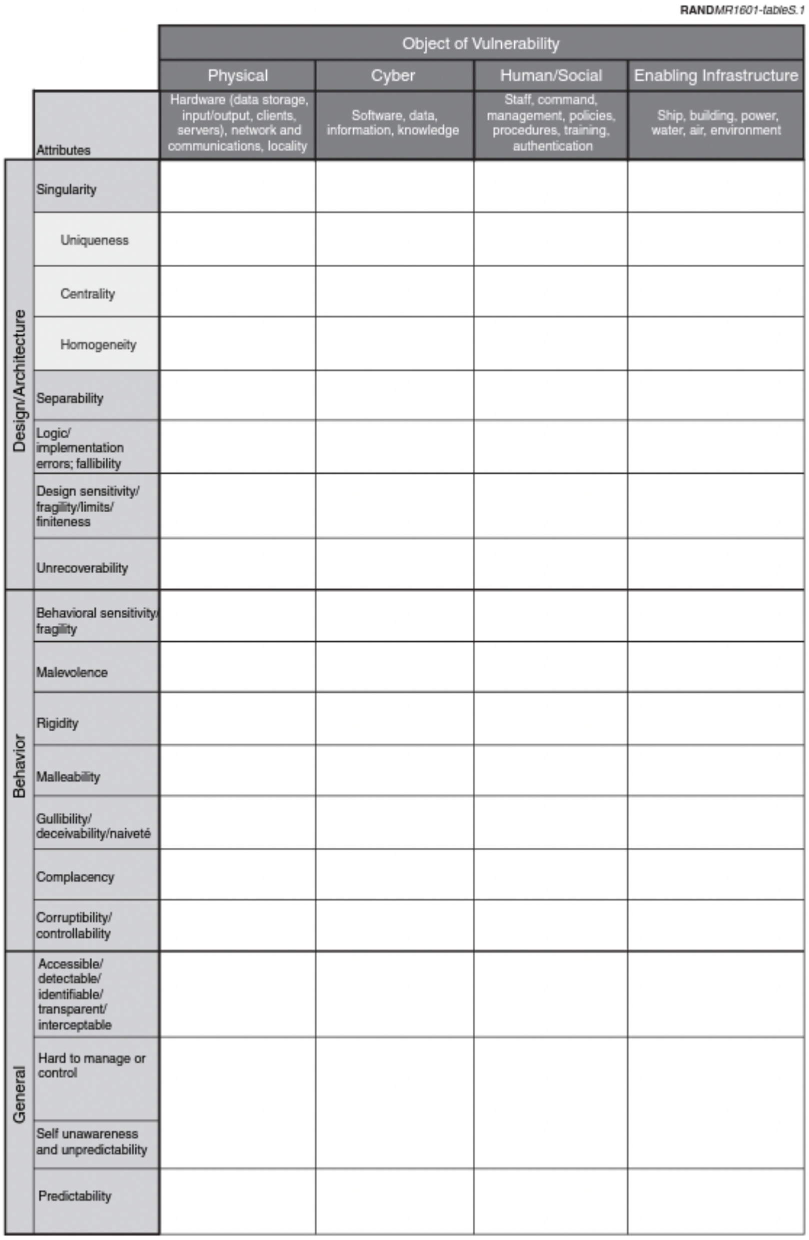
- Identify your organization's essential information *functions*.
- Identify essential information *systems* that implement these functions.
- Identify *vulnerabilities* of these systems.
- Identify pertinent *security techniques* to mitigate these vulnerabilities.
- *Select and apply* techniques based on constraints, costs, and benefits.
- *Test* for robustness and actual feasibilities under threat.[64]

VAM provides a matrix that guides analysts through a review of vulnerabilities across various information system attributes (see Figure 14). The objects of vulnerability include not only cyber considerations, but also physical, human/social, and enabling infrastructure. The methodology aims to identify both known and exploited vulnerabilities as well as existing vulnerabilities that have yet to be encountered or exploited.[65]

[63] Philip S. Antón et al., "The Vulnerability Assessment & Mitigation Methodology: Finding and Fixing Vulnerabilities in Information Systems," ed. National Defense Research Institute (Santa Monica, Calif.: Rand, 2003), xv–xvi.

[64] Antón et al., xv–xvi.

[65] Antón et al., xv.



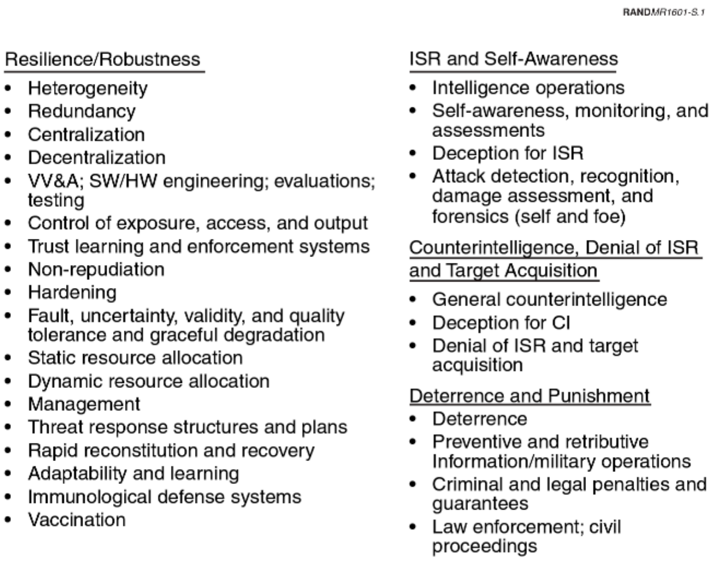
RANDMR1601-tableS.1

		Object of Vulnerability			
		Physical	Cyber	Human/Social	Enabling Infrastructure
	Attributes	Hardware (data storage, input/output, clients, servers), network and communications, locality	Software, data, information, knowledge	Staff, command, management, policies, procedures, training, authentication	Ship, building, power, water, air, environment
Design/Architecture	Singularity				
	Uniqueness				
	Centrality				
	Homogeneity				
	Separability				
	Logic/ implementation errors; fallibility				
	Design sensitivity/ fragility/limits/ finiteness				
	Unrecoverability				
Behavior	Behavioral sensitivity/ fragility				
	Malevolence				
	Rigidity				
	Malleability				
	Gullibility/ deceivability/naiveté				
	Complacency				
	Corruptibility/ controllability				
General	Accessible/ detectable/ identifiable/ transparent/ interceptable				
	Hard to manage or control				
	Self unawareness and unpredictability				
	Predictability				

Figure 14. VAM Vulnerability Matrix[66]

VAM also provides several resources to identify and evaluate security mitigation techniques to address identified vulnerabilities. The list of available security techniques is in Figure 15.

[66] Antón et al., xvii.



RANDMR1601-S.1

Resilience/Robustness

- Heterogeneity
- Redundancy
- Centralization
- Decentralization
- VV&A; SW/HW engineering; evaluations; testing
- Control of exposure, access, and output
- Trust learning and enforcement systems
- Non-repudiation
- Hardening
- Fault, uncertainty, validity, and quality tolerance and graceful degradation
- Static resource allocation
- Dynamic resource allocation
- Management
- Threat response structures and plans
- Rapid reconstitution and recovery
- Adaptability and learning
- Immunological defense systems
- Vaccination

ISR and Self-Awareness

- Intelligence operations
- Self-awareness, monitoring, and assessments
- Deception for ISR
- Attack detection, recognition, damage assessment, and forensics (self and foe)

Counterintelligence, Denial of ISR and Target Acquisition

- General counterintelligence
- Deception for CI
- Denial of ISR and target acquisition

Deterrence and Punishment

- Deterrence
- Preventive and retributive Information/military operations
- Criminal and legal penalties and guarantees
- Law enforcement; civil proceedings

Figure 15. VAM Security Mitigation Techniques[67]

VAM provides a matrix to map each vulnerability to the security mitigation techniques. Values in the matrix indicate whether each technique is a primary or secondary candidate for mitigating the vulnerability (2 and 1), can incur additional vulnerabilities implemented (-1 and -2), and when a vulnerability actually facilitates security techniques (0).[68] Figure 16 shows an excerpt of this matrix.

[67] Antón et al., xviii.

[68] Antón et al., 51–52.

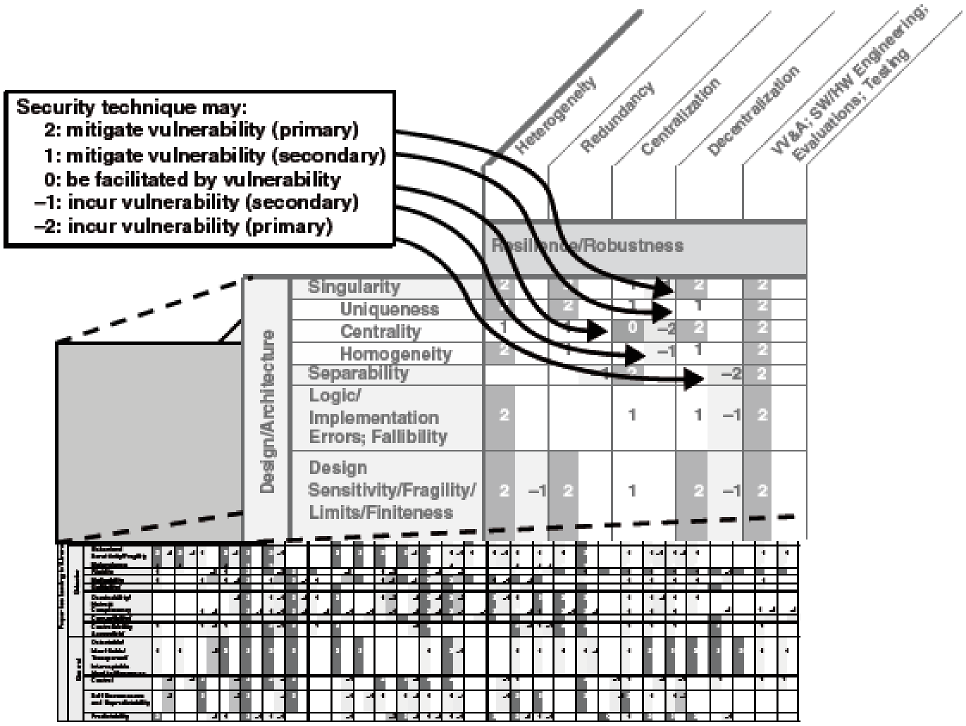

Security technique may:
2: mitigate vulnerability (primary)
1: mitigate vulnerability (secondary)
0: be facilitated by vulnerability
–1: incur vulnerability (secondary)
–2: incur vulnerability (primary)
Heterogeneity
Redundancy
Centralization
Decentralization
VV&A; SW/HW Engineering; Evaluations; Testing
Resilience/Robustness
Design/Architecture
Singularity
Uniqueness
Centrality
Homogeneity
Separability
Logic/ Implementation Errors; Fallibility
Design Sensitivity/Fragility/ Limits/Finiteness

Figure 16. Values Relating Vulnerabilities to Security Techniques in VAM[69]

RAND acknowledges that the matrix in Figure 16 will identify many potential security techniques for each vulnerability. Thus, VAM provides filtering approaches based on the job role of the evaluator conducting the security assessment and the stages of an attack.[70] Taken together, these filters focus attention on the attack stages in which "the evaluator has more ability to implement protections and countermeasures."[71] The attack stage analysis is of particular interest for this report.

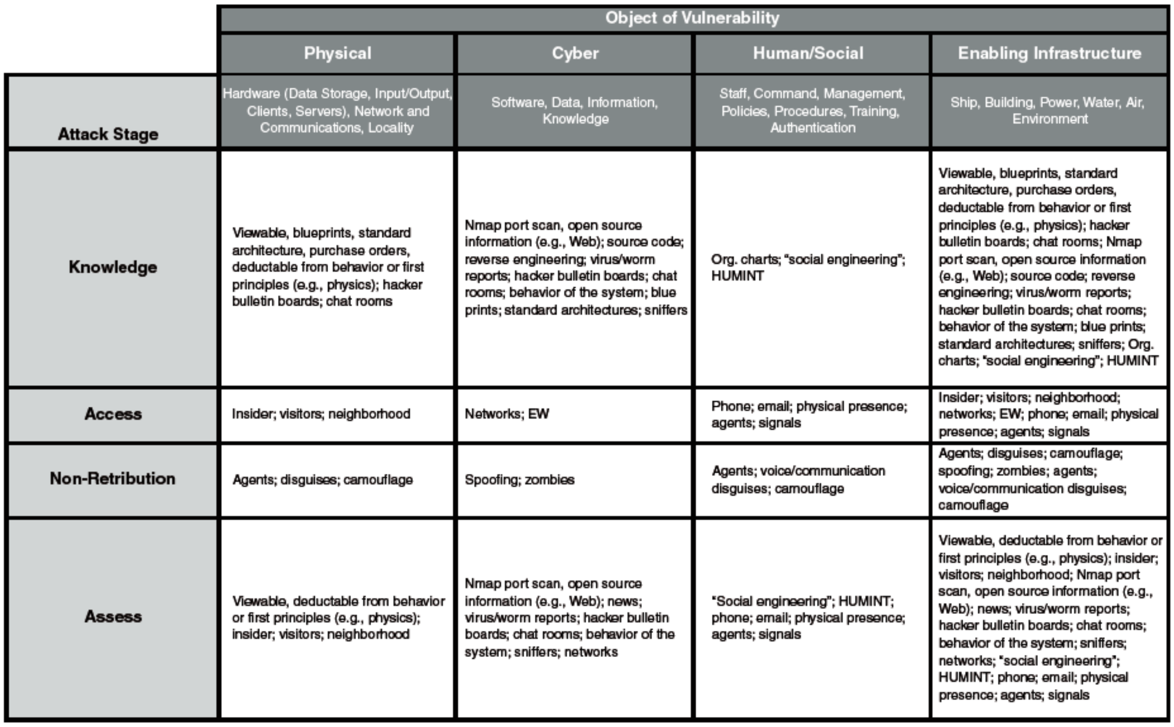
This filtering technique begins by identifying the following stages of an attack: knowledge, access, target vulnerability, non-retribution, and the ability to assess the success of an attack. As with a traditional kill chain analysis, VAM assumes that complete prevention of any one of the first three components will deny a successful attack. VAM stipulates that the four and fifth components are not critical to the success of an attack but are "so important to many attackers that an attack can be prevented if these components are denied."[72] Figure 17 lists the major ways that an attacker can accomplish each component of an attack. Figure 18 identifies which vulnerability properties can be exploited in each of the five attack stages.

[69] Antón et al., 51.

[70] Antón et al., 54.

[71] Antón et al., 57.

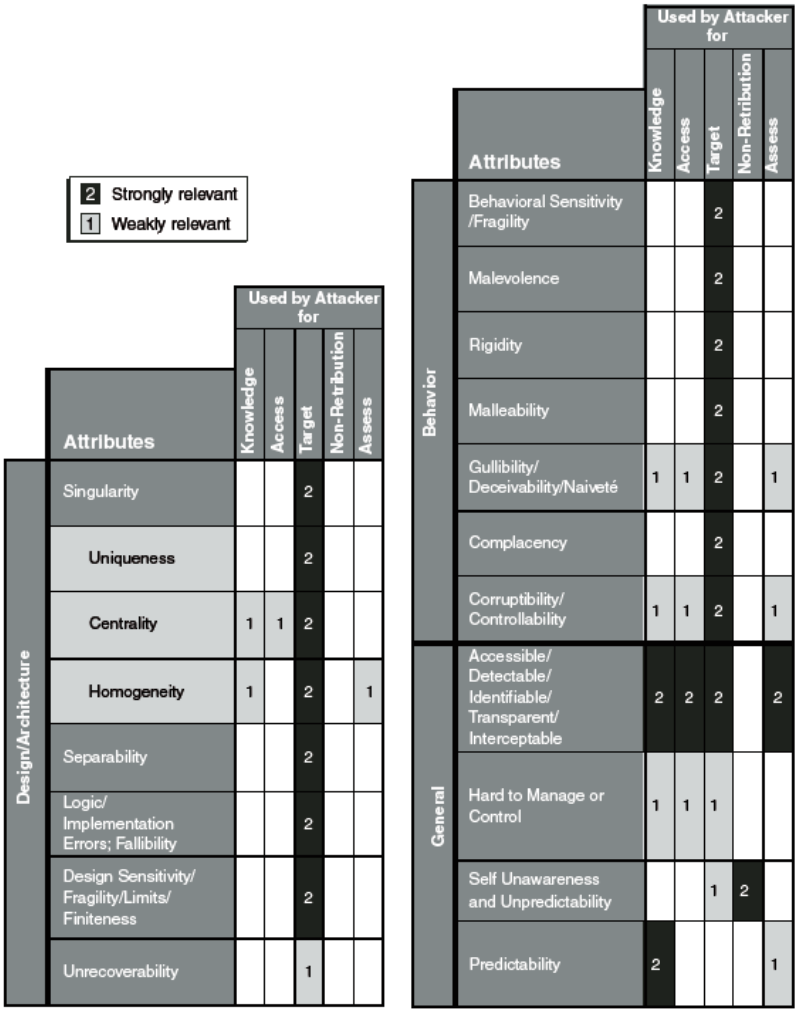
[72] Antón et al., 56–57.



	Object of Vulnerability			
	Physical	Cyber	Human/Social	Enabling Infrastructure
Attack Stage	Hardware (Data Storage, Input/Output, Clients, Servers), Network and Communications, Locality	Software, Data, Information, Knowledge	Staff, Command, Management, Policies, Procedures, Training, Authentication	Ship, Building, Power, Water, Air, Environment
Knowledge	Viewable, blueprints, standard architecture, purchase orders, deductable from behavior or first principles (e.g., physics); hacker bulletin boards; chat rooms	Nmap port scan, open source information (e.g., Web); source code; reverse engineering; virus/worm reports; hacker bulletin boards; chat rooms; behavior of the system; blue prints; standard architectures; sniffers	Org. charts; "social engineering"; HUMINT	Viewable, blueprints, standard architecture, purchase orders, deductable from behavior or first principles (e.g., physics); hacker bulletin boards; chat rooms; Nmap port scan, open source information (e.g., Web); source code; reverse engineering; virus/worm reports; hacker bulletin boards; chat rooms; behavior of the system; blue prints; standard architectures; sniffers; Org. charts; "social engineering"; HUMINT
Access	Insider; visitors; neighborhood	Networks; EW	Phone; email; physical presence; agents; signals	Insider; visitors; neighborhood; networks; EW; phone; email; physical presence; agents; signals
Non-Retribution	Agents; disguises; camouflage	Spoofing; zombies	Agents; voice/communication disguises; camouflage	Agents; disguises; camouflage; spoofing; zombies; agents; voice/communication disguises; camouflage
Assess	Viewable, deductable from behavior or first principles (e.g., physics); insider; visitors; neighborhood	Nmap port scan, open source information (e.g., Web); news; virus/worm reports; hacker bulletin boards; chat rooms; behavior of the system; sniffers; networks	"Social engineering"; HUMINT; phone; email; physical presence; agents; signals	Viewable, deductable from behavior or first principles (e.g., physics); insider; visitors; neighborhood; Nmap port scan, open source information (e.g., Web); news; virus/worm reports; hacker bulletin boards; chat rooms; behavior of the system; sniffers; networks; "social engineering"; HUMINT; phone; email; physical presence; agents; signals

Figure 17. Methods for Accomplishing Each Component of an Attack in VAM[73]

[73] Antón et al., 58.



2 Strongly relevant
1 Weakly relevant

	Attributes	Used by Attacker for				
		Knowledge	Access	Target	Non-Retribution	Assess
Design/Architecture	Singularity			2		
	Uniqueness			2		
	Centrality	1	1	2		
	Homogeneity	1		2		1
	Separability			2		
	Logic/ Implementation Errors; Fallibility			2		
	Design Sensitivity/ Fragility/Limits/ Finiteness			2		
	Unrecoverability			1		

	Attributes	Used by Attacker for				
		Knowledge	Access	Target	Non-Retribution	Assess
Behavior	Behavioral Sensitivity /Fragility			2		
	Malevolence			2		
	Rigidity			2		
	Malleability			2		
	Gullibility/ Deceivability/Naiveté	1	1	2		1
	Complacency			2		
	Corruptibility/ Controllability	1	1	2		1
General	Accessible/ Detectable/ Identifiable/ Transparent/ Interceptable	2	2	2		2
	Hard to Manage or Control	1	1	1		
	Self Unawareness and Unpredictability			1	2	
	Predictability	2				1

Figure 18. Vulnerability Exploitation by Attack Component in VAM[74]

Although it focuses solely on information systems and includes objects of vulnerability outside the scope of this study (e.g. cyber, human social, etc.), there are many aspects of RAND VAM that could be instructive to developers of a physical attack framework. Potentially useful components include: the consideration of physical objects of vulnerability for various system attributes, the robust list of mitigation options mapped to each vulnerability, the breakdown of attack stages, the list of physical techniques for accomplishing each stage of an attack, and the mapping of system attributes to attack stages.

2.12 Chemical Facility Anti-Terrorism Standards (CFATS) Process[75]

Congress gave the Department of Security (DHS) regulatory authority over security at high-risk chemical facilities in the Homeland Security Appropriations Act of 2007 (P.L. 109-295). In

[74] Antón et al., 60.

[75] CFATS authority lapsed as of 7/28/2023. Please visit https://www.cisa.gov/resources-tools/programs/chemical-facility-anti-terrorism-standards-cfats for future updates to CFATS.

response, DHS developed the Chemical Facility Anti-Terrorism Standards (CFATS), which outline the requirements that high-risk chemical facilities must meet to comply with the Act. Among other things, CFATS established "eighteen Risk-Based Performance Standards (RBPSs) that identify the areas for which a facility's security posture will be examined, such as perimeter security, access control, personnel surety, and cyber security."[76]

Facilities across all critical infrastructure sectors are required to follow CFATS if in possession of certain chemicals of interest that are above a screening threshold quantity as defined in CFATS documentation. The purpose of CFATS is to ensure that any facility identified by CISA, who administers CFATS for DHS, as high-risk "has sufficient security measures in place to reduce the risks associated with its [chemical of interest]."[77] Facilities submit an initial review survey via CISA's Chemical Security Assessment Tool (CSAT) and if deemed high-risk are assigned a tier and directed to complete a Security Vulnerability Assessment and a Site Security Plan or an Alternative Security Program plan. If the security plan satisfies CFATS regulations, the facility receives a Letter of Authorization followed by an Authorization Inspection from a CISA Chemical Security Inspector. Following successful completion of these steps, the facility will receive a Letter of Approval and will be visited by a CISA Inspector for reoccurring compliance inspections. An overview of the CFATS process is provided in Figure 19.[78]

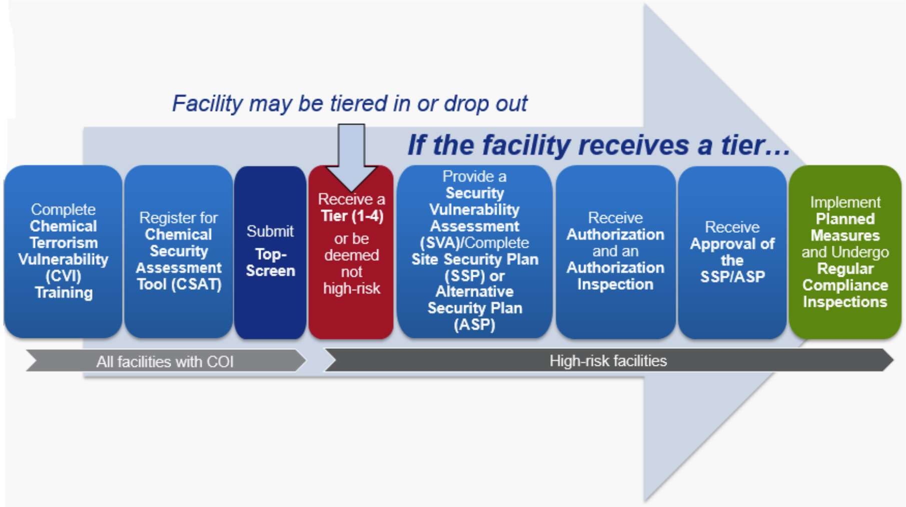

Facility may be tiered in or drop out
If the facility receives a tier…
Complete Chemical Terrorism Vulnerability (CVI) Training
Register for Chemical Security Assessment Tool (CSAT)
Submit Top-Screen
Receive a Tier (1-4) or be deemed not high-risk
Provide a Security Vulnerability Assessment (SVA)/Complete Site Security Plan (SSP) or Alternative Security Plan (ASP)
Receive Authorization and an Authorization Inspection
Receive Approval of the SSP/ASP
Implement Planned Measures and Undergo Regular Compliance Inspections
All facilities with COI
High-risk facilities

Figure 19. CFATS Process Steps[79]

The Security Vulnerability Assessment is used to "identify the facility's use of chemicals of interest (COI), critical assets, and measures related to the facility's policies, procedures, and

[76] "Risk-Based Performance Standards Guidance - Chemical Facility Anti-Terrorism Standards" (Washington, D.C.: Infrastructure Security Compliance Division, Cybersecurity and Infrastructure Security Agency, May 2009), 8, www.cisa.gov/publication/cfats-rbps-guidance.

[77] "Chemical Facility Anti-Terrorism Standards (CFATS) Process | CISA," accessed July 18, 2023, https://www.cisa.gov/resources-tools/programs/chemical-facility-anti-terrorism-standards-cfats/cfats-process.

[78] "Chemical Facility Anti-Terrorism Standards (CFATS) Process | CISA."

[79] "Chemical Facility Anti-Terrorism Standards (CFATS) Process | CISA."

resources that are necessary to support the facility's security plan."[80] A critical asset is "an asset whose theft, diversion, loss, damage, disruption, or degradation would result in a significant adverse impact to human life, national security, or a critical economic asset."[81] The wide range of critical assets include but are not limited to physical security (such as personnel, security infrastructure, security procedures), physical safety infrastructure (i.e. for managing safety and emergency response measures), cyber systems involved in the management of processes and security, vessels, containers, and equipment used in the transportation and storage of materials, and personnel who manage security and safety risks.[82]

Facilities submit the Security Vulnerability Assessment through CSAT and are then required to complete an online Site Security Plan questionnaire to further describe existing or planned security measures.[83] The CSAT-based questionnaire is accompanied by the "CFATS Risk-Based Performance Standards Guidance," which describes each risk-based performance standard and provides examples of various security measures that meet the required levels.[84] Facilities can elect to submit an Alternative Security Program plan instead of the Site Security Plan, which allows a facility to use its own template to address CFATS requirements.

Upon completion of these steps, a Chemical Security Inspector will visit the facility to verify the content of the plan and ensure the facility is following the appropriate safety and security measures.[85] The Chemical Security Inspector provides resource guides, fact sheets, and additional information addressing commonly asked questions for storing high risk chemicals onsite. Because CFATS is sector agnostic and applies to both public and private facilities, facility staff may vary in their familiarity with hazardous chemicals, vulnerability, risks, and underlying security.[86] A unique benefit of the individual site visits is that the inspectors can customize the risk information they share based on individual stakeholder needs.[87]

2.13 DISARM

DISARM is "the open-source, master framework for fighting disinformation through sharing data [and] analysis, and coordinating effective action."[88] The framework became available for use in 2019 and is modeled after MITRE ATT&CK, building upon the matrix structure of tactics, techniques, and procedures.[89] Work started on DISARM in 2017 and was developed by a number

[80] "Chemical Security Assessment Tool (CSAT) Security Vulnerability Assessment (SVA) and Site Security Plan (SSP) | CISA," accessed July 18, 2023, https://www.cisa.gov/resources-tools/programs/chemical-facility-anti-terrorism-standards-cfats/chemical-security-assessment-tool-csat/security-vulnerability-assessment-and-site-security-plan.

[81] "Chemical Security Assessment Tool (CSAT) Security Vulnerability Assessment (SVA) and Site Security Plan (SSP) | CISA."

[82] "Chemical Security Assessment Tool (CSAT) Security Vulnerability Assessment (SVA) and Site Security Plan (SSP) | CISA."

[83] "Chemical Security Assessment Tool (CSAT) Security Vulnerability Assessment (SVA) and Site Security Plan (SSP) | CISA."

[84] "Risk-Based Performance Standards Guidance - Chemical Facility Anti-Terrorism Standards," 8.

[85] "Chemical Facility Anti-Terrorism Standards (CFATS) Process | CISA."

[86] Based on interviews with stakeholders conducted on March 28, 2023

[87] Based on interviews with stakeholders conducted on March 28, 2023

[88] "DISARM Framework," DISARM Framework, accessed July 18, 2023, https://www.disarm.foundation/framework.

[89] "DISARM Framework" and "DISARM Disinformation TTP (Tactics, Techniques and Procedures) Framework," Jupyter Notebook (2022; repr., DISARM Foundation, July 17, 2023), https://github.com/DISARMFoundation/DISARMframeworks.

of stakeholders, including the MITRE Corporation, and with community input.[90] The open-source format of the framework encourages users to share data, best practices, and analysis to help others learn effective mitigation strategies.[91] The DISARM Foundation, created in late 2021, currently maintains, enhances, and promotes the DISARM framework.[92]

DISARM is composed of two separate frameworks: one to describe the creation of a disinformation incident from the perspective of an adversary and the other to explore potential defense response techniques from the defender perspective.[93] The framework has been used internationally by the European Union, the United Nations, and NATO. The World Health Organization also used DISARM to address anti-vaccination disinformation campaigns in Europe.[94]

3 Use Cases for a Physical Attack Framework

The next phase of this study focused on developing relevant use cases for a physical attack framework based on research and feedback from stakeholders. In identifying the use cases, the project team considered the ways in which a physical attack framework could be used in various physical security settings, agnostic of critical infrastructure sector or facility type. Additionally, the project team considered how a physical attack framework could be used in conjunction with MITRE ATT&CK to assess combined cyber-physical attack paths.

The project team identified three general use case categories: evaluation of an existing security plan, generation of scenarios, and information sharing. Additional details are described in the sections that follow.

3.1 Use Case – Evaluate an Existing Security Plan

3.1.1 Evaluate Security Plan Comprehensiveness

Analysts or security personnel could use a physical attack framework to assess whether a facility has mitigations, protections, or procedures in place to address each of the relevant TTPs an adversary could use in an attack. This assessment could be used to identify gaps in security plans and/or areas where the plan should be strengthened. The results could also be combined with a risk assessment methodology—which would measure the risk reduction resulting from proposed new security measures—or a cost-benefit analysis methodology to prioritize the options identified. LLNL's Stack Switchboard is an example of a tool that already exists in the cyber domain that uses MITRE ATT&CK to assess an existing security plan's ability to address known cyber attack

[90] "DISARM Foundation - A Brief History of DISARM," DISARM Foundation, accessed July 31, 2023, https://www.disarm.foundation/brief-history-of-disarm and "DISARM Disinformation TTP (Tactics, Techniques and Procedures) Framework."

[91] "DISARM Disinformation TTP (Tactics, Techniques and Procedures) Framework."

[92] "DISARM Foundation - About Us," accessed July 18, 2023, https://www.disarm.foundation/about-us.

[93] "Disarm Framework Explorer."

[94] "DISARM Framework."

TTPs. A physical attack framework with a similar TTP matrix structure could be incorporated into Stack Switchboard to extend the tool's capabilities into the physical domain.

3.1.2 Evaluate Value of New Security Mitigations

A physical attack framework could also be used to assess the value of deploying new mitigation efforts, by determining whether the new mitigations would address additional TTPs. Using the framework in this way would allow analysts or security personnel to evaluate whether proposed mitigations improve the comprehensiveness of a security plan. Again, this could be combined with a risk assessment methodology to evaluate the potential risk reduction. As in the previous case, LLNL's Stack Switchboard is an example of a tool that currently assists security personnel in evaluating whether/which additional mitigation efforts will address additional cyber TTPs and could be extended into the physical domain with the help of a physical attack framework.

3.1.3 Categorize and Track Observed Occurrences

A physical attack framework could also be used to categorize and track observed or suspected security incidents by mapping them against the framework's TTPs. The resulting data set could assist analysts or security personnel in identifying discernible patterns, emerging trends, and unusual incidents that standout among typical occurrences. For example, a sudden spike in a particular TTP could indicate the emergence of a new threat actor or trend among existing threat actors. Likewise, the repeated use of a particular TTP among many facilities in a particular area or sector could alert analysts that isolated incidents may part of a larger pattern that should be addressed. A physical attack framework could also provide potential mitigations for response.

Such a data set does not necessarily have to be started anew. For example, the University of Maryland's Study of Terrorism and Response to Terrorism (START) data repository contains multiple datasets that categorize real world occurrences based on threat actor, target sector, and method of attack (physical and cyber).[95] Various law enforcement and government agencies also maintain information on security incidents. These data sets could incorporate the TTP structure contained in a physical attack framework to add additional detail and utility to existing repositories.

CISA has underscored the importance of the categorization and tracking of adversary TTPs in the cyber domain, by partnering with the Homeland Security Systems Engineering and Development Institute™ and the MITRE ATT&CK team to develop Decider. Decider is a tool for stakeholders to map observed adversary behavior more easily to the MITRE ATT&CK® framework. CISA had also previously published a *Best Practices for MITRE ATT&CK® Mapping* guide. Per CISA, "Decider helps network defenders, analysts, and researchers quickly and accurately map adversary tactics, techniques, and procedures (TTPs) to the ATT&CK knowledge base. ATT&CK has been adopted by CISA and network defenders worldwide because it helps cyber threat intelligence (CTI) analysts and others understand adversary behaviors."[96]

[95] "START- National Consortium for the Study of Terrorism and Response to Terrorism," Data and Tools, accessed August 1, 2023, https://www.start.umd.edu/data-and-tools/start-datasets.

[96] "Decider - A Tool for Network Defenders, Analysts, and Researchers Working with MITRE ATT&CK" (CISA, March 2023), 1, https://www.cisa.gov/sites/default/files/2023-03/decider_fact_sheet_508c.pdf.

3.2 Use Case – Generate Scenarios

3.2.1 Generate Consistent Potential Attack Paths for a Particular Facility

Using the TTPs in a physical attack framework, analysts or security personnel could generate plausible attack paths tailored to the mitigations in place at a particular facility. The attack paths could then be used to test existing security plans against potential attack scenarios. This could enable security personnel to identify security gaps and consider appropriate mitigation options to address them.

Using the TTPs in a physical attack framework as building blocks for the generation of attack paths could also enable researchers to generate attack scenarios at scale. Scenario generation is the foundation for many types of risk analysis but can be prohibitively complex and time consuming to do at scale without automation. By providing a structured and consistent set of TPPs, a physical attack framework could enable such automation.

LLNL's Pathway Enumeration Tool (PET), for example, automatically enumerates credible and self-consistent cyber attack scenarios that lead to consequences of interest. PET leverages both the SANS Industrial Control Systems (ICS) Cyber Kill Chain and the MITRE ATT&CK Framework for Enterprise and ICS networks. PET can automatically generate hundreds or thousands of realistic and credible cyber attack scenarios.[97] A physical attack framework could enable PET, or similar analytic tools, to generate scenarios for physical attacks. When combined with cyber attack generation capabilities, PET could also produce combined cyber-physical attack paths—significantly improving the ability to conduct analysis in support of cyber and physical security convergence.

3.2.2 Generate Potential Attack Paths for Adversary Profiles, Based on Capability Levels

The TTPs in a physical attack framework could each be categorized according to the type of adversary capable of carrying them out. This could be done using broad actor tiers (ranging from, e.g., casual individual actor to professional criminal organization to full-scope nation state) or specific adversary groups based on known capabilities (via open-source reporting or intelligence). Such a categorization could be used to filter attack paths by a given adversary/adversary category. Analysts and security personnel could use this information to gain a better understanding of their risk profile against various types of adversaries. This information could also provide a better understanding of potential security vulnerabilities given specific threat or intelligence information, if available.

In the cyber domain, MITRE includes a listing of "groups" within the ATT&CK data set. MITRE defines groups as "activity clusters that are tracked by a common name in the security community" and notes that "[a]nalysts track these clusters using various analytic methodologies and terms such as threat groups, activity groups, and threat actors." Information about each group includes techniques and software used.[98]

LLNL has developed generic but well-defined adversary tiers that it has used in conjunction with its Quantitative Intelligent Adversary Risk Assessment (QIARA) scenario difficulty scoring

[97] Mike Nygaard, Jovana Helms, and Chloe Applegate, "Cyber Design Basis Threat" (Lawrence Livermore National Laboratory, November 12, 2021), 2.

[98] "MITRE ATT&CK®," Groups, accessed August 1, 2023, https://attack.mitre.org/groups/.

methodology and PET to analyze which adversary tiers are capable of which attack paths. This analysis has then been used to support estimates of the probability and potential consequences of attacks by adversary tier.

Physical attack simulation tools such as LLNL's Joint Conflict and Tactical Simulation (JCATS) could also be used in conjunction with adversary- or adversary tier-specific attack paths. If specific threat information is known, the specific attacks paths could be simulated against different mitigation efforts in JCATS, providing statistical results to support decision making on response options.

3.3 Use Case – Information Sharing

3.3.1 Establish a Common Language for Information Sharing

A physical attack framework could establish a common language with which to characterize physical threats and incidents to improve information sharing throughout the physical security community. The framework could be used to draft and release consistent and easily understood information on security incidents; on adversaries, capabilities, and associated attack paths; and to recommended security improvements across organizations.

Facilitating the sharing of information in a commonly understood manner not only improves communication but also aids in the creation of consistent datasets, enables analytic tools to be used across fields, and helps users more easily describe attributes of physical attack TTPs. MITRE ATT&CK and DISARM are both examples in which security personnel, researchers, government agencies and organization, and companies use similar frameworks for information sharing across users and communities.

3.3.2 Evaluate A Security Plan against Known Incidents or Adversaries

When an attack occurs or new information on adversary intent, tactics, or techniques is identified, it may be important to share critical information with at risk sectors or facilities. Under these conditions, clarity and timeliness are critical and it is often helpful if actionable next steps can be included. As discussed above, a physical attack framework can provide a common language that enables information sharing. By tying mitigations to TTPs, it can also quickly provide relevant mitigation options that can help security professionals develop action plans, particularly when time is of the essence. This is useful for organizations like CISA, who routinely push this type of information out to critical infrastructure stakeholders, as well as for individual facilities, who could use TTP-based information to identify security gaps and evaluate their own readiness. For longer-term planning, analysts or security personnel could use this type of information in conjunction with a risk assessment methodology to prioritize areas for security investments.

Security professionals currently use MITRE ATT&CK as a reference tool to aid in incident response and to stay up to date on the latest adversary groups, incidents, and TTPs.[99] CISA highlights the importance of ATT&CK's information sharing role in the release of its Decider tool:

[99] See, e.g., Brandon Min, "A Primer on MITRE ATT&CK as an Incident Response Framework," Panther, accessed August 1, 2023, https://panther.com/cyber-explained/mitre-attack-framework-incident-response/. and "Role of MITRE ATT&CK Framework in Incident Response," CYWARE, October 11, 2021, https://cyware.com/security-guides/incident-response/role-of-mitre-attck-framework-in-incident-response-e1e7.

> By making ATT&CK mapping easier, Decider helps users more quickly and accurately understand adversary activities. After obtaining accurate mappings, users can move on to many other ATT&CK activities, including…[s]haring the findings with others by publishing threat intelligence reports…[and] discovering mitigations that help prevent techniques from working in the first place.[100]

A physical attack framework could be a valuable tool by which information is shared about known threat actors and physical TTPs targeting specific critical infrastructure.

4 Requirements for a Physical Attack Framework

Using the lessons learned from the literature review and stakeholder feedback, the project team next developed a series of requirements for a physical attack framework, ensuring it meets the needs of each of the use cases outlined in the previous section. The requirements address elements related to the framework's scope, data needs, and structure.

4.1 Requirements – Scope

The scope of a physical attack framework should include TTPs that span the entire physical attack path, ranging from at least reconnaissance to impact. While MITRE ATT&CK does not include adversary TTPs that take place after the attack has occurred, as RAND VAM notes, "post-boom" actions—such as escaping without being identified or maintaining the ability to assess whether the attack was successful—may be important to the attacker and should be considered for inclusion in a physical attack framework.[101] As in ATT&CK, a physical attack framework should allow for movement in any order across the matrix and for the omission of tactics altogether.

The TTPs in a physical attack framework should be general enough to be applicable to many different stakeholders, facilities, applications, and attack types. They should be described with a level of detail that allows for users to understand their meaning, while allowing for customization for specific use cases. If needed, a physical attack framework could include separate matrices for different types of sectors or facilities—similar to ATT&CK's enterprise, mobile, and ICS.

In addition to high-level tactics, a physical attack framework should include supporting information such as techniques, sub-techniques, and procedure examples. It should also include a list of mitigations and potentially means of detection that are mapped to the techniques for ease of reference. Additionally, a physical attack framework should consider maintaining a list of relevant adversary groups, weapons, and attacks/campaigns.

4.2 Requirements – Data Needs

The data included in a physical attack framework should be based on observed or feasible events. Physical attack analysts or administrators should review potential data inputs to ensure the validity of the details and information before it is included in the framework. Like MITRE ATT&CK, all

[100] "Decider - A Tool for Network Defenders, Analysts, and Researchers Working with MITRE ATT&CK," 1.

[101] Antón et al., "The Vulnerability Assessment & Mitigation Methodology: Finding and Fixing Vulnerabilities in Information Systems," 56–57.

data should be based on open-source, reliable incident reports, threat intelligence, etc. or publicly available research on new techniques that "closely align" with common adversary actions.[102] All data sources should be clearly cited and linked, when possible, in the framework.

A physical attack framework should also include a mechanism for users to submit data or feedback for review. An analyst or administrator for the framework should review all user-submitted data to determine validity, relevancy, and applicability.

4.3 Requirements – Structure

A physical attack framework should include a matrix of TTPs, similar to MITRE ATT&CK. A matrix structure would allow for interoperability between a physical attack framework and ATT&CK, creating opportunities for analysis of combined cyber-physical attack paths. Feedback from stakeholder interviews underscored that using a familiar design can increase the ease of use and adoption amongst potential users.[103] DISARM provides one example of a framework that leverages the TTP structure of ATT&CK.[104] The use of a similar structure would also enable integration of a physical attack framework into tools that currently use MITRE ATT&CK (such as LLNL's Stack Switchboard and PET).

The physical attack matrix of TTPs should be written in plain language with commonly used physical security terminology. The use of plain language would ease adoption, understanding, and communication across sectors.

5 Key Findings and Recommendations

Based on the information gathered from the literature review, engagement with stakeholders, and evaluation of the use cases against identified requirements, this study identified the following six key findings and recommendations:

- There is a need for a new physical attack characterization framework.
- A physical attack framework should be interoperable with the MITRE ATT&CK framework.
- A physical attack framework should be broadly applicable, but with detailed tactics, techniques, and procedures that encompass the entire attack path.
- A physical attack framework should be based on observed or feasible events.
- A physical attack framework should adapt features from existing methodologies, frameworks, and taxonomies.
- A physical attack framework should be owned, overseen, and maintained by one organization.

[102] "FAQ | MITRE ATT&CK®."

[103] Based on interviews with stakeholders conducted on May 16, 2023

[104] "DISARM Framework Explorer," August 7, 2023, https://disarmframework.herokuapp.com/.

Each finding and associated recommendation is discussed in additional detail below.

5.1 Key Finding 1: There Is a Need for a New Physical Attack Framework

A novel physical attack framework is needed for the characterization of physical attacks agnostic of facility type or sector. Physical attack taxonomies, methodologies, and other tools for evaluating physical security do exist—as found in the literature review and through engagement with key stakeholders—across a variety of organizations, sectors, and fields. However, they tend to be limited to a specific critical infrastructure sector or facility type (e.g. ATTP 3-39.32, UFC: DoD Minimum Antiterrorism Standards for Buildings, NNSA SD 470.4-2, and the CFATS process) or are more focused on security or vulnerability assessment instead of the characterization of attacks themselves (e.g. CARVER, MSHARPP, RAND VAM, IST with PMI and RMI, SAFE).

5.2 Key Finding 2: A Physical Attack Framework Should Be Interoperable with the MITRE ATT&CK Framework

To best support analysis related to cyber and physical security convergence, a physical attack framework should be interoperable with MITRE ATT&CK. Interoperability will allow a physical attack framework to be incorporated more easily into tools, methods, and research areas where MITRE ATT&CK is already deployed. Interoperability between the two frameworks could also encourage adopters of a physical attack framework to explore the use of MITRE ATT&CK as they expand their efforts around cyber and physical security convergence.

5.3 Key Finding 3: A Physical Attack Framework Should Be Broadly Applicable, with Detailed Tactics, Techniques, and Procedures that Encompass the Entire Attack Path

A physical attack framework should include TTPs that can apply to a wide range of physical attack scenarios regardless of critical infrastructure sector, facility type, threat actor, or weapon used. It is also critical that the framework encompass the entire attack path to ensure that all relevant TTPs are considered and cataloged. While a broad scope is necessary, like MITRE ATT&CK, the framework should also include sufficient detail for users to fully understand and differentiate between each TTP. Narrative descriptions, real-world examples, explanations of how each TTP may apply to different facility types, and other supporting information are useful in ensuring each TTP is sufficiently described.

While the high-level tactics in MITRE ATT&CK (i.e. Initial Access, Execution, Impact, etc.) are broadly applicable to physical attacks, developers of a physical attack framework should use the resources identified in Section 2 to identify gaps and update descriptions (see additional detail on this in Section 5.5 below). Developers should also consider whether they would like to expand the scope of MITRE ATT&CK beyond impact to actions such as escape tactics, that may be more relevant in physical attacks than in cyber.

The use of multiple matrices for different types of sectors or facilities may be useful but should only be used if necessary. As with MITRE ATT&CK, the physical attack matrix should not require that all tactics be used in the analysis of a given attack or that they be used in a particular order. In addition to TTPs, a physical attack framework should include mitigations and potentially should include means of detection and lists of relevant adversary groups, weapons, and attacks/campaigns.

To increase applicability and adoption, the TTPs and accompanying narrative should be written using plain language or commonly-used physical security terminology. Terms and descriptions already contained in the physical attack frameworks discussed in Section 2 provide a useful starting place. Technical jargon may be unavoidable, but when used, should be thoroughly explained. The addition of a glossary, such as those referenced or included in ATTP 3-39.32, the UFC: DoD Minimum Antiterrorism Standards for Buildings, and NSA SD 470.4-2 should be considered.[105] Developers of a physical attack framework should also review methodologies such as DBT or the CARVER matrix, which have been used extensively outside of their primary user groups (i.e. the nuclear security community and the military, respectively) as examples of how straightforward concepts can encourage wide adoption.

5.4 Key Finding 4: A Physical Attack Framework Should Be Based on Observed or Feasible Events

The data and research used to create and update a physical attack matrix should be sourced from either observed incidents in the real world or scenarios that are based on historical events with feasible escalations. The framework should include both low-probability and high-probability scenarios, without veering into "science fiction." Like MITRE ATT&CK, all data should be based on reliable, publicly-available incident reports, threat intelligence, etc. or publicly available research on new techniques that closely align with common adversary actions. All data should be reviewed by administrators before inclusion.[106]

Validated data from existing, trusted frameworks and databases—such as the University of Maryland's START data—may be incorporated into the physical attack framework where possible and applicable. This can help create more efficient data updates by providing consistently structured, vetted pipelines for updated data that are regularly refreshed.

All data in the framework should be clearly cited. The framework should also include options for users to submit data or feedback. Both MITRE ATT&CK and DISARM provide examples of how to collect user-submitted information.[107]

5.5 Key Finding 5: A Physical Attack Framework Should Adapt Features from Existing Methodologies, Taxonomies, and Frameworks

While no existing method or tool fully fits the requirements for a physical attack framework, there are lessons to be learned, models to follow, and data to be leveraged from both the physical and cyber domains. Thus, the project team recommends that a physical attack framework should adapt key features from existing methodologies, taxonomies, tools, and frameworks. Specific recommendations are described in the following sub-sections.

5.5.1 Detailing Tactics, Techniques, and Procedures

MITRE ATT&CK details a set of tactics and techniques a cyber adversary would use to accomplish certain goals. This broad list encompasses the entire attack path and is a comprehensive

[105] "Physical Security," August 2010, Glossary-1; "Unified Facilities Criteria (UFC) - DoD Minimum Antiterrorism Standards for Buildings," December 12, 2018, 8; and "Enterprise Safeguards and Security Planning and Analysis Program," 11.

[106] "FAQ | MITRE ATT&CK®."

[107] "DISARM Disinformation TTP (Tactics, Techniques and Procedures) Framework" and "MITRE ATT&CK®," Contribute, accessed August 3, 2023, https://attack.mitre.org/resources/contribute/.

starting point for a physical attack framework TTP matrix. Table 1 provides a general example of how tactics and adversary goals broadly defined in MITRE ATT&CK could be adapted for a physical attack framework.

Table 1. Tactics and Adversary Goals, Adapted from Cyber to Physical

MITRE ATT&CK TACTICS AND GOALS		
Tactic	**Cyber Attack Adversary Goals**[108]	**Physical Attack Adversary Goals** (*indicates where the goals are altered)
Reconnaissance	Gather information they can use to plan future operations	Gather information they can use to plan future operations
Resource Development	Establish resources they can use to support operations	Establish resources they can use to support operations
Initial Access	Get into your network	Get into your facility*
Execution	Run malicious code	Exploit a vulnerability*
Persistence	Maintain their foothold	Maintain entry*
Privilege Escalation	Gain higher-level permissions	Escalate level of access*
Defense Evasion	Avoid being detected	Avoid being detected
Credential Access	Steal account names and passwords	Steal/gather entry-dependent locks and keys*
Discovery	Figure out your environment	Explore access for additional vulnerabilities*
Lateral Movement	Move through your environment	Move through your environment
Collection	Gather data of interest to their goal	Gather information, materials, tools relevant to goal*
Command and Control	Communicate with compromised systems to control them	N/A
Exfiltration	Steal data	Steal or execute attack at desired target*
Impact	Manipulate, interrupt, or destroy your systems and data	Destroy, damage, or cause chaos to environment*

In addition to the TTPs contained in MITRE ATT&CK, many other frameworks reviewed in the literature review contain information that could contribute to the development of a physical attack matrix. RAND VAM lists the stages of attack and the major ways that an attacker can accomplish

[108] "What Is the MITRE ATT&CK Framework?" Palo Alto Networks, accessed July 18, 2023, https://origin-www.paloaltonetworks.com/cyberpedia/what-is-mitre-attack-framework.

each stage.[109] ATTP 3-39.32 contains examples of adversary TTPs throughout the document.[110] The UFC: DoD Minimum Antiterrorism Standards for Buildings includes attack and weapon types that could be useful in the creation of TTPs.[111] NNSA SD 470.4-2 contains guidance on sabotage analysis and scenario development that could also contribute to TTP creation.[112] Developers of a physical attack matrix could also collect specific DBT documents from various critical infrastructure sectors and use the adversary characterizations contained in the DBTs to potentially extrapolate TTPs.

The literature review also identified many examples of vulnerability or security assessment methodologies.[113] While most of these do not contain adversary TTPs outright, the vulnerability and security criteria they ask analysts to consider can be adapted to TTPs. For example, the "accessibility" criteria in both the CARVER and MSHARPP matrices examine how easily an attacker can access a facility (or the critical systems within that facility), what defenses or mitigations are present, etc.[114] These criteria could help the developer of a physical attack framework support the need for an *initial access* tactic within a physical attack matrix and provide a structure for brainstorming specific techniques to facilitate access.

Likewise, the extensive question set included in the IST can assist in the development of a physical attack framework by ensuring it includes a comprehensive set of TTPs that span the range of security considerations include in the IST. The CFATS security vulnerability assessment can be used similarly.

5.5.2 Addressing Mitigation Techniques

MITRE ATT&CK includes a mitigation matrix that maps techniques to mitigations, as seen in Figure 20. A physical attack framework should include a similar mitigation matrix, with the goal of including at least one mitigation for every technique.

[109] Antón et al., "The Vulnerability Assessment & Mitigation Methodology: Finding and Fixing Vulnerabilities in Information Systems."

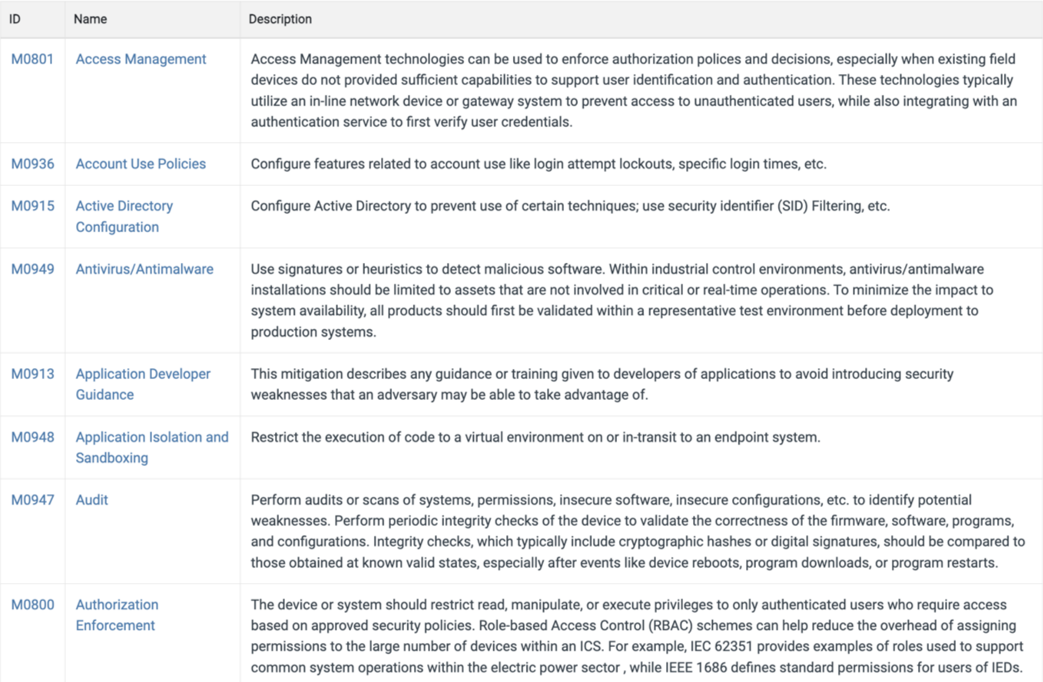
[110] "Physical Security."

[111] "Unified Facilities Criteria (UFC) - DoD Minimum Antiterrorism Standards for Buildings," December 12, 2018, 15.

[112] "Enterprise Safeguards and Security Planning and Analysis Program," 2–6.

[113] These include CARVER, MSHARPP, IST/PMI/RMI, SAFE, NNSA, RAND VAM, and CFATS.

[114] See, e.g., "Police Intelligence Operations," 5-18–20.



ID	Name	Description
M0801	Access Management	Access Management technologies can be used to enforce authorization polices and decisions, especially when existing field devices do not provided sufficient capabilities to support user identification and authentication. These technologies typically utilize an in-line network device or gateway system to prevent access to unauthenticated users, while also integrating with an authentication service to first verify user credentials.
M0936	Account Use Policies	Configure features related to account use like login attempt lockouts, specific login times, etc.
M0915	Active Directory Configuration	Configure Active Directory to prevent use of certain techniques; use security identifier (SID) Filtering, etc.
M0949	Antivirus/Antimalware	Use signatures or heuristics to detect malicious software. Within industrial control environments, antivirus/antimalware installations should be limited to assets that are not involved in critical or real-time operations. To minimize the impact to system availability, all products should first be validated within a representative test environment before deployment to production systems.
M0913	Application Developer Guidance	This mitigation describes any guidance or training given to developers of applications to avoid introducing security weaknesses that an adversary may be able to take advantage of.
M0948	Application Isolation and Sandboxing	Restrict the execution of code to a virtual environment on or in-transit to an endpoint system.
M0947	Audit	Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses. Perform periodic integrity checks of the device to validate the correctness of the firmware, software, programs, and configurations. Integrity checks, which typically include cryptographic hashes or digital signatures, should be compared to those obtained at known valid states, especially after events like device reboots, program downloads, or program restarts.
M0800	Authorization Enforcement	The device or system should restrict read, manipulate, or execute privileges to only authenticated users who require access based on approved security policies. Role-based Access Control (RBAC) schemes can help reduce the overhead of assigning permissions to the large number of devices within an ICS. For example, IEC 62351 provides examples of roles used to support common system operations within the electric power sector , while IEEE 1686 defines standard permissions for users of IEDs.

Figure 20. Examples of MITRE ATT&CK for ICS Mitigations (where ID is the technique addressed by each mitigation)[115]

Many of the resources discussed in the literature review contain mitigations that could be leveraged directly in a physical attack framework. RAND VAM includes a list of security mitigation techniques that can be mapped to specific vulnerabilities and filtered by the stages of an attack.[116] The guidance in ATTP-3-39.32 covers security aspects to consider during site design, including mitigation efforts to increase the physical security of a site.[117] Basic mitigation tips that address CARVER criteria are provided in ATTP 3-39.20.[118] The CFATS Site Security Plan is accompanied by the "CFATS Risk-Based Performance Standards Guidance," which provides examples of various security measures that meet the required security levels.[119] In the IST, questions are categorized according to the type of infrastructure and security policy they cover (i.e. lighting, access control, and security plans). Based on the answers submitted by the security advisor(s), facilities are provided with "Vulnerabilities and Options for Consideration" (VOFCs) related to identified gaps and weaknesses, which can be used to generate mitigations in a physical attack framework.[120] The UFC: DoD Minimum Antiterrorism Standards for Buildings include a robust set of standards meant to protect DoD facilities from a variety of physical attacks.[121]

[115] "Mitigations - ICS | MITRE ATT&CK®," accessed July 18, 2023, https://attack.mitre.org/mitigations/ics/.

[116] Antón et al., "The Vulnerability Assessment & Mitigation Methodology: Finding and Fixing Vulnerabilities in Information Systems," xvii, 51–52.

[117] "Physical Security," v-vi.

[118] "Police Intelligence Operations," 5-18–20.

[119] "Risk-Based Performance Standards Guidance - Chemical Facility Anti-Terrorism Standards," 8.

[120] Based on interviews with stakeholders conducted on May 16, 2023

[121] "Unified Facilities Criteria (UFC) - DoD Minimum Antiterrorism Standards for Buildings," December 12, 2018.

The literature review also yielded several tools, standards, and directives that, while not providing specific mitigations, contain information that can be used by developers of a physical attack matrix to extrapolate mitigations. MSHARPP and NNSA SD 470.4-2, for example, both provide a structure for enumerating vulnerabilities, which analysts can use to brainstorm associated mitigations.

5.5.3 Adapting Familiar Structures

The MITRE ATT&CK TTP matrix structure is now well known and serves as the basis of analytic tools and capabilities throughout the cyber security community (including several at LLNL). As discussed previously, leveraging the familiar matrix design and TTP structure would increase initial user familiarity with a physical attack framework, ease adoption, and allow for interoperability with ATT&CK.

Although DISARM is entirely focused on misinformation and not physical security threats, it is a successful example of interdisciplinary collaboration to create a user-friendly framework based on the ATT&CK structure. The final DISARM frameworks are structured in a tactic-technique matrix like ATT&CK, through with an additional layer to more broadly group tactics into planning, preparation, execution, and assessment categories, and with content relevant to their subject matter.[122] DISARM also adds additional tactics to assess the cognitive impacts on the population stemming from a disinformation campaign.[123] A physical attack framework could similarly leverage the ATT&CK structure while adding, adapting, and replacing content to meet the needs of the physical attack community.

5.6 Key Finding 6: A Physical Attack Framework Should Be Owned, Overseen, and Maintained by One Organization

A physical attack framework should be owned, overseen, and maintained by one organization. Discussions with multiple physical security stakeholders identified areas in methodologies where proper record keeping, maintenance, and information sharing was key to their success.[124] As discussed in previous sections, data oversight, change management, review, and updates are necessary to maintain a consistent, reliable, and accurate physical attack framework. To accomplish these, a dedicated owner, who can also ensure that adequate funding and staffing is maintained, is needed. MITRE ATT&CK and DISARM provide different ownership models, but both underscore the need for a single management team. Although they are managed by a single group, both ATT&CK and DISARM actively encourage input and feedback by their stakeholders.[125]

[122] “DISARM Framework Explorer.”

[123] S Terp and P Breuer, “DISARM: A Framework for Analysis of Disinformation Campaigns” (IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA), Salerno, Italy: IEEE, 2022), 1–8, https://doi.org/10.1109/CogSIMA54611.2022.9830669.

[124] Based on interviews with LLNL stakeholders conducted during March through April 2023.

[125] “MITRE ATT&CK®” and “DISARM Disinformation TTP (Tactics, Techniques and Procedures) Framework.”

6 Summary and Recommendations for Future Work

In this study, the project team reviewed existing physical security taxonomies and assessment methodologies and identified use cases, requirements, and recommendations for the development and maintenance of a physical attack framework. Next steps should focus on the creation of an initial framework, using the examples and suggestions provided in this paper. After an initial draft has been developed, the framework should be tested against a range of attack types and sectors/facilities to ensure it is applicable to the full scope of physical attacks and infrastructures. It should also be tested for interoperability with the MITRE ATT&CK matrix, by applying it to combined cyber-physical scenarios and tools. Opportunities for obtaining feedback and input from the physical security community should also be pursued. Concurrently, a sustainable management structure for the framework should be identified to ensure it can be properly updated and maintained as new data becomes available.

With the growth of the cyber attack surface, it is increasingly necessary to not only understand cyber defense but also to understand the interplay between cyber and physical security. A physical attack framework, which allows for characterization of physical attack paths and works seamlessly with ATT&CK, will provide analysts and security professionals with a critical tool for understanding new and emerging attack opportunities and for developing and sharing mitigations throughout the critical infrastructure community.