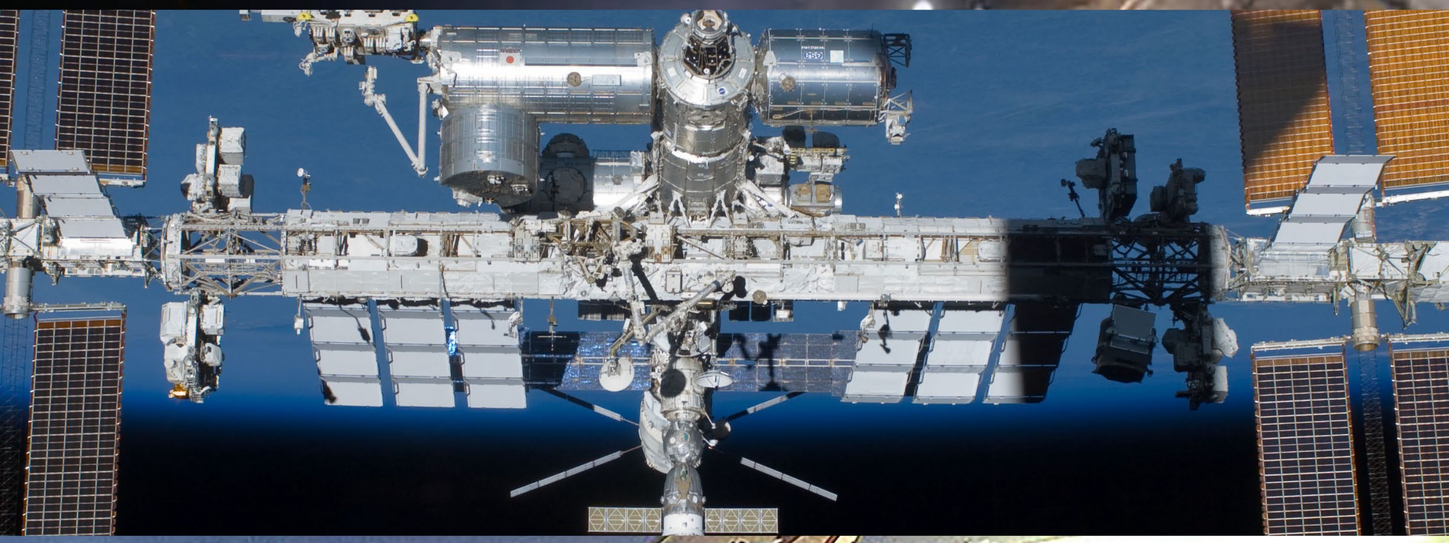
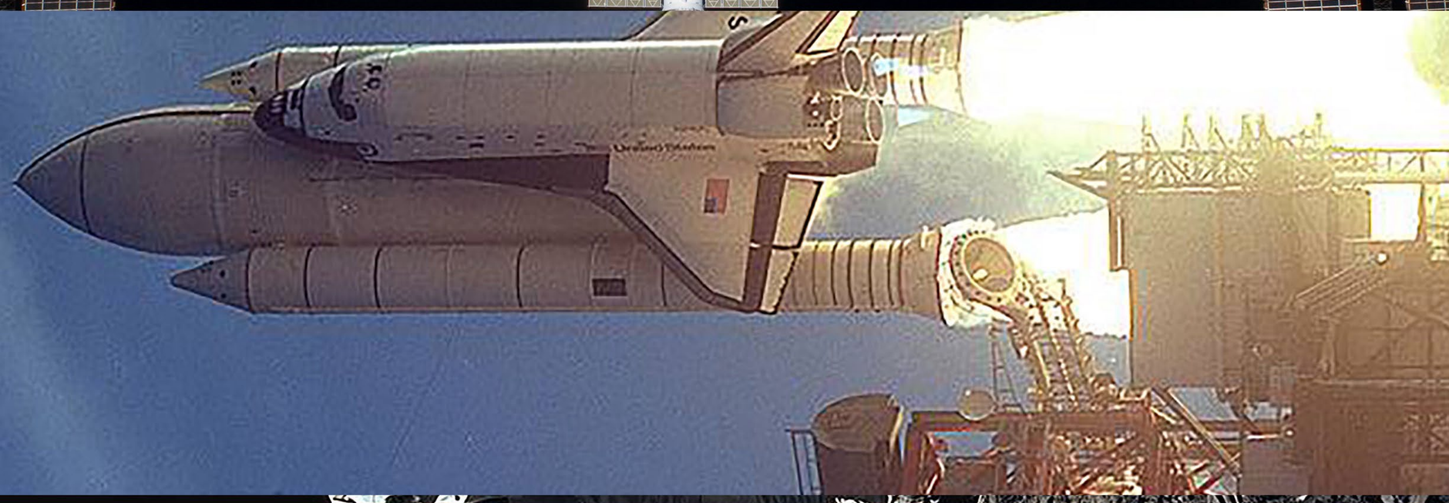




Space Law, AI, and Cybersecurity

Protecting the Security and Sustainability of the Next Frontier

Texas Bar Computer and Technology Section

Charles Lee Mudd Jr.

April 27, 2023

NIST Cybersecurity Framework

Framework Launched 2014

Updated 2018

MUDD LAW

SPACE | INTERNET | CREATIVES | IP | STARTUPS

NIST Cybersecurity Framework

Before a Cyber Attack or Intrusion

NIST Cybersecurity Framework

Core Tiers Profiles

MUDD LAW

SPACE | INTERNET | CREATIVES | IP | STARTUPS

NIST Cybersecurity Framework

Before a Cyber Attack or Intrusion

NIST Cybersecurity Framework - Core

Functions, Categories, Sub-Categories, Informative References

MUDD LAW

SPACE | INTERNET | CREATIVES | IP | STARTUPS

NIST Cybersecurity Framework

Before a Cyber Attack or Intrusion

NIST Cybersecurity Framework – Core | Functions

Identify, Protect, Detect, Respond, Recover

MUDD LAW

SPACE | INTERNET | CREATIVES | IP | STARTUPS

NIST Cybersecurity Framework

Before a Cyber Attack or Intrusion

NIST Cybersecurity Framework – Core | Categories

Subsets of Functions (Asset Management, Risk Assessment)

MUDD LAW

SPACE | INTERNET | CREATIVES | IP | STARTUPS

Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

NIST Cybersecurity Framework

Before a Cyber Attack or Intrusion

NIST Cybersecurity Framework – Core | Sub-Categories

Subsets of Categories (detection notifications investigated)

MUDD LAW

SPACE | INTERNET | CREATIVES | IP | STARTUPS

NIST Cybersecurity Framework

Before a Cyber Attack or Intrusion

NIST Cybersecurity Framework – Core | References

Resources to Guide Sub-Categories

MUDD LAW

SPACE | INTERNET | CREATIVES | IP | STARTUPS

Table 2: Framework Core

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	**CIS CSC** 12 **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	**CIS CSC** 13, 14 **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/IEC 27001:2013** A.8.2.1 **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and	**CIS CSC** 17, 19 **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03


August 2022
Workshop #1
4,000+ attendees
100 countries
February 2023
Workshop #2
2,000 attendees
69 countries
February 2023
Working Sessions
~250 attendees
Fall 2023
Workshop #3
2022
COMMUNITY ENGAGEMENT
2024
February 2022
NIST Cybersecurity RFI
April 2022
130+ RFI Comments received
June 2022
RFI Analysis
September 2022
Workshop Analysis
January 2023
Concept Paper
April 2023
Core Draft
March 2023
~ 100 Comments received
Summer 2023
Draft
Comments
Early 2024
CSF 2.0

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

Search

Topics | Spotlight | Resources & Tools | News & Events | Careers | About | REPORT A CYBER ISSUE

Home / Resources & Tools / Groups

SHARE:

Resources & Tools

- All Resources & Tools
- Services
- Programs
- Resources
- Training
- **Groups**

Space Systems Critical Infrastructure Working Group

Critical Infrastructure Security and Resilience

Return to top

Topics | Spotlight | Resources & Tools | News & Events | Careers | About

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

888-282-0870 Central@cisa.dhs.gov

MUDD LAW

SPACE | INTERNET | CREATIVES | IP | STARTUPS

New Developments

2022 – Cyber Incident Reporting for Critical Infrastructure Act

Part of Consolidated Appropriations Act of 2022

Amends Homeland Security Act

MUDD LAW
SPACE | INTERNET | CREATIVES | IP | STARTUPS

New Developments

2022 – Cyber Incident Reporting for Critical Infrastructure Act

Critical Infrastructure Sectors (16)

Communications Sector

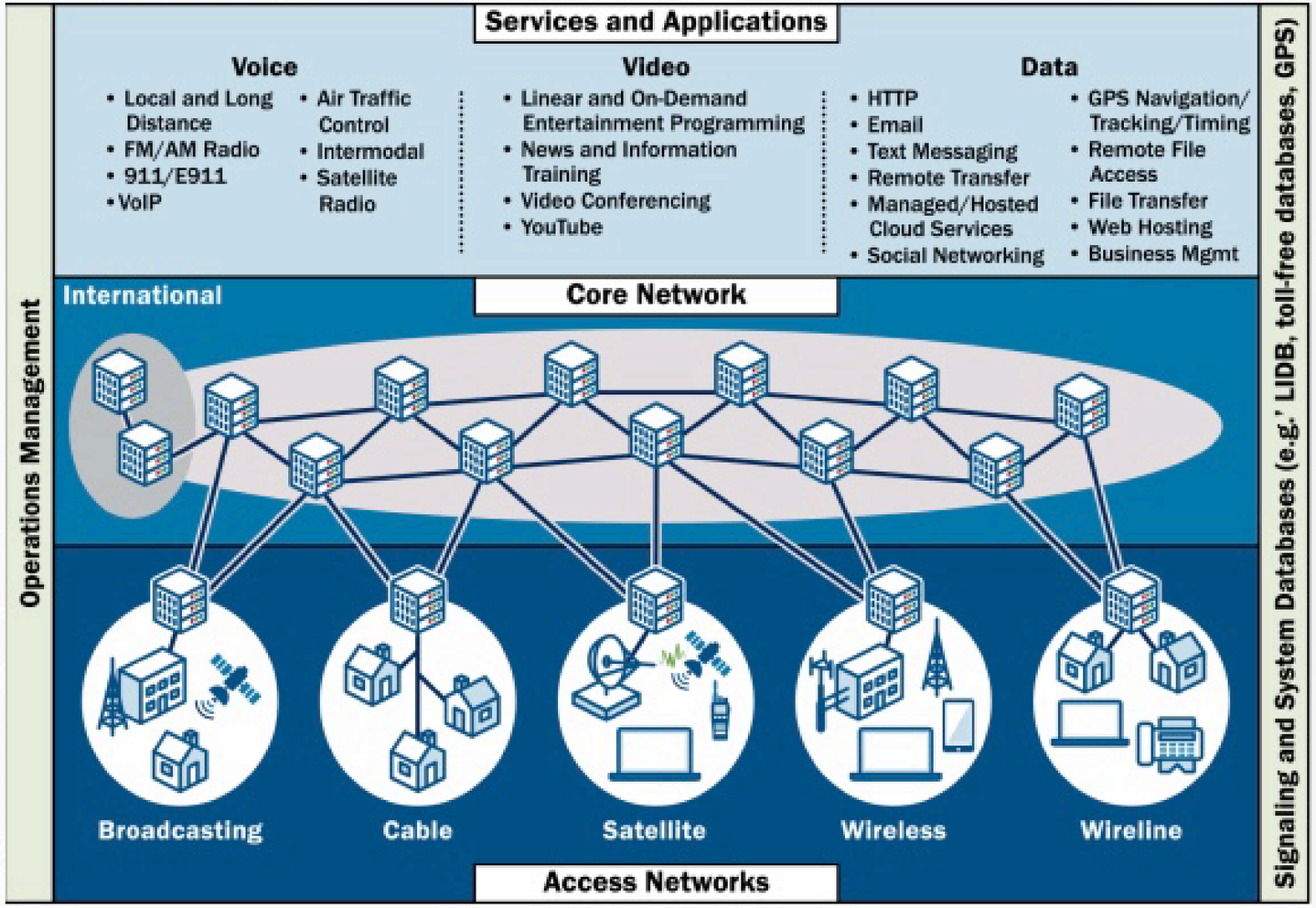
Energy | IT | Financial Services | Emergency Services | Transportation

MUDD LAW

SPACE | INTERNET | CREATIVES | IP | STARTUPS

"Communications Sector is one of the few sectors that can affect all other sectors"

Cybersecurity & Infrastructure Security Agency (2021)



New Developments

CISA Communications Sector

Broadcast | Cable | Satellite | Wireless | Wireline

CIRCIA – Reporting Requirements

MUDD LAW

SPACE | INTERNET | CREATIVES | IP | STARTUPS

New Developments

CIRCIA

CISA Rulemaking

March 2024 NPRM Target

Final Rule 18 Months

MUDD LAW

SPACE | INTERNET | CREATIVES | IP | STARTUPS

New Developments

CIRCIA

Compliance with Final Rule

Suggest Now

report@cisa.gov or (888) 282-0870

MUDD LAW

SPACE | INTERNET | CREATIVES | IP | STARTUPS

Space Assets

Earth Stations

Space Stations

Connection Between Stations

MUDD LAW

SPACE | INTERNET | CREATIVES | IP | STARTUPS

Businessweek

The Satellite Hack Everyone Is Finally Talking About

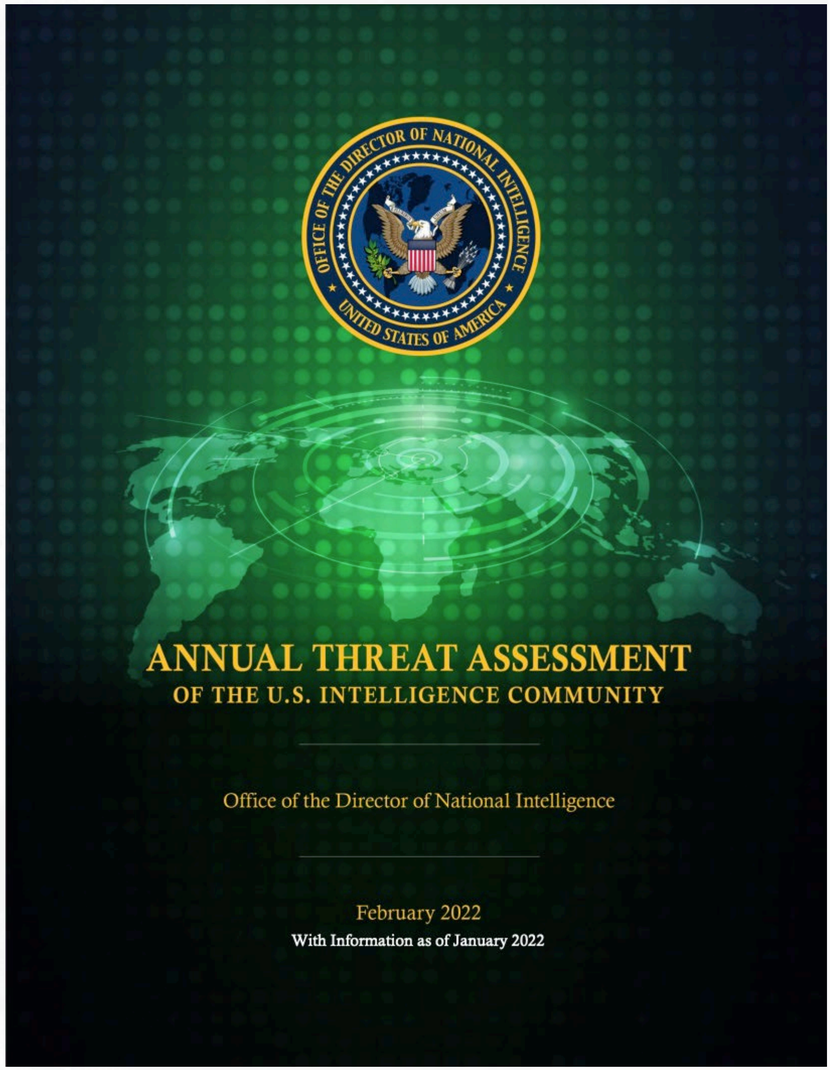
As Putin began his invasion of Ukraine, a network used throughout Europe—and by the Ukrainian military—faced an unprecedented cyberattack that doubled as an industrywide wake-up call.

By Katrina Manson
Illustrations by Jordan Speer
March 1, 2023 at 12:01 AM CST

Share this article

Gift this article

Cybersecurity and Space



Cybersecurity and Space

China

"We assess that China presents the broadest, most active, and persistent cyber espionage threat to U.S. Government and private sector networks. China's cyber pursuits and export of related technologies increase the threats of attacks against the U.S. homeland, suppression of U.S. web content that Beijing views as threatening to its control, and the expansion of technology-driven authoritarianism globally."

Cybersecurity and Space

Russia

“We assess that Russia will remain a top cyber threat as it refines and employs its espionage, influence, and attack capabilities. We assess that Russia views cyber disruptions as a foreign policy lever to shape other countries’ decisions, as well as a deterrence and military tool.”

Cybersecurity and Space

Iran

“Iran’s growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of U.S. and allied networks and data.”

Cybersecurity and Space

North Korea

“North Korea’s cyber program poses a sophisticated and agile espionage, cybercrime, and attack threat. Pyongyang is well positioned to conduct surprise cyber attacks given its stealth and history of bold action.”

Types of Attacks

Spoofing | Interception | Corruption | Tampering

Denial of Service | Brute-Force

Signal Hijacking | SSA Deception | Seizure of Control

Jamming | Solar Storms

MUDD LAW

SPACE | INTERNET | CREATIVES | IP | STARTUPS

Recommendations

Secure methods for authentication (MFA)

Enforce principle of least privilege

Review trust relationships

Recommendations

Encryption

Ensure Robust Patching and System Configuration Audits

Monitor at Ingress and Egress Points (logs)

Ensure Incident Response, Resilience, and Continuity of Operations

Recommendations

Assess:

Presence of Insecure Remote Access Tools
(Telnet, ftp, SSH, SCP, VNC)

Network Traffic from SATCOM networks to other networks

Recommendations

Assess:

Unauthorized use of local or backup accounts within SATCOM

Unexpected terminal to terminal traffic

Brute force login attempts

Recommendations

Where to Begin?

Passwords and Password Policy

MFA

Recommendations

Where to Begin?

Read Materials

NIST, CISA, Space Sector Specific

Monitor Developments

MUDD LAW

SPACE | INTERNET | CREATIVES | IP | STARTUPS

DOC – NOAA - CRSRA

Final Rules – May 19, 2020

Cybersecurity

(eg tracking, telemetry, and control)

encryption

DOC – NOAA - CRSRA

Final Rules – May 19, 2020

Cybersecurity

recommend taking higher level, provide for encryption of data where possible

DOC – NOAA - CRSRA

Final Rules – May 19, 2020

Cybersecurity

Recommendations Provided

(Requirements less stringent that had been proposed)

Recommendations

Where to Begin?

Identify Asset Vulnerabilities

Identify Vulnerabilities

Know Your Partners

You Have An Obligation To Know Your Customers and Partners

This essentially means that you should understand the nuances of any company with whom you work.

Recommendations

Where to Begin?

Allow Only Authorized Devices to Communicate with Satellites

Authenticate Device

Drop All Unconfirmed Communications

Check Integrity of Communications

MUDD LAW

SPACE | INTERNET | CREATIVES | IP | STARTUPS

Recommendations

Where to Begin?

Scale Up: Allow Only Authorized Devices to Access Sensitive Data

Encryption

Authenticated Before Decryption

But Encryption All Around

MUDD LAW

SPACE | INTERNET | CREATIVES | IP | STARTUPS

Recommendations

Where to Begin?

Make Satellites Resilient to Adverse Conditions

Solid Protocols

Alternate or Secondary Communications Channel

When down, store data and send afterwards

MUDD LAW

SPACE | INTERNET | CREATIVES | IP | STARTUPS

Recommendations

Where to Begin?

Build Protections Into Satellite

Thwart DDOS and Other Attacks

Protect Vehicle if Communications Compromised

Enhance Ability to Ingest and Share Threat Data

Compliance by Design

MUDD LAW

SPACE | INTERNET | CREATIVES | IP | STARTUPS

Recommendations

Design

Secure Device Design and Development

Hardware, Firmware, OS, and Apps

Redundancy

Recommendations

Design

Hardware Root of Trust and Secure Boot

Provide Update, Upgrade, and Uninstall Capabilities

Avoid Known Security Weaknesses

Prevent Unauthorized Software from Executing

Recommendations

Design

Log

Investigate

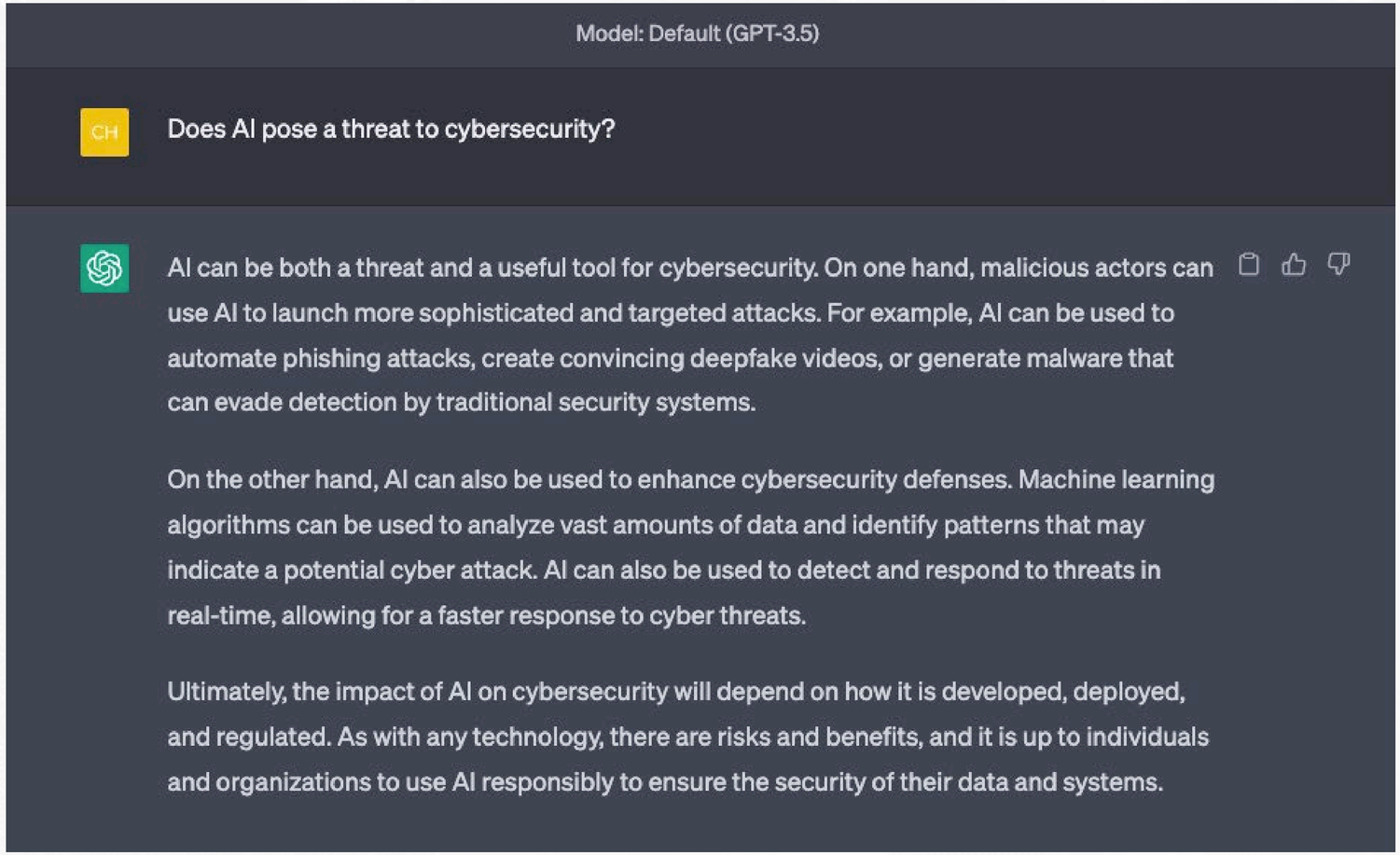
Prevent

Recover

MUDD LAW

SPACE | INTERNET | CREATIVES | IP | STARTUPS

AI


Model: Default (GPT-3.5)
CH
Does AI pose a threat to cybersecurity?
AI can be both a threat and a useful tool for cybersecurity. On one hand, malicious actors can use AI to launch more sophisticated and targeted attacks. For example, AI can be used to automate phishing attacks, create convincing deepfake videos, or generate malware that can evade detection by traditional security systems.
On the other hand, AI can also be used to enhance cybersecurity defenses. Machine learning algorithms can be used to analyze vast amounts of data and identify patterns that may indicate a potential cyber attack. AI can also be used to detect and respond to threats in real-time, allowing for a faster response to cyber threats.
Ultimately, the impact of AI on cybersecurity will depend on how it is developed, deployed, and regulated. As with any technology, there are risks and benefits, and it is up to individuals and organizations to use AI responsibly to ensure the security of their data and systems.

Circle Back to Law Firms

LAW360 | Pulse

Small Law

THURSDAY, APRIL 27, 2023

Exclusive

Chicago Law Firm Hit With Security Incident

By Steven Lerner

A small Chicago-based law firm has been struck by a security incident involving possible unauthorized access to an email account, Law360 Pulse learned exclusively on Thursday.

Read full article » | Save to favorites »

Connection Accepted
Connection Refused - Policy violation
Connection Refused - Policy violation
Connection Refused - Policy violation
Connection Refused - Policy violation
Connection Refused - Policy violation
Connection Refused - Policy violation
Connection Refused - Policy violation
Connection Refused - Policy violation
Connection Accepted
Connection Accepted
Connection Accepted
Connection Accepted
Connection Accepted
Connection Accepted
Blocked - IP Spoofing
Blocked - IP Spoofing
Connection Refused - Policy violation
Connection Refused - Policy violation
Connection Accepted
Connection Accepted
Connection Accepted
Connection Accepted

Additional Resources

CISA (cisa.org)

NIST (nist.gov) 1.1 | 2.0

Introduction to Cybersecurity for Commercial Space Operations (2/22)
https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8270-draft2.pdf

MUDD LAW

SPACE | INTERNET | CREATIVES | IP | STARTUPS

Questions and Comments

Charles Lee Mudd Jr.
411 S. Sangamon Street
Suite 1B
Chicago, Illinois 606
312.964.5051
312.803.1667
@clmuddjr
charles@muddlaw.com
muddlaw.com

mlo.bz/