SUNS

Software Understanding for National Security

SUNS Partnership Forum 2025 (SPF-25) Report

Douglas Ghormley
Christopher Harrison
Sandia National Laboratories
May 13, 2025

https://suns.sandia.gov/
suns@sandia.gov

U.S. DEPARTMENT OF ENERGY
NNSA

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

SAND2025-05642PE

Introductions

Dr. Douglas Ghormley, Sandia National Laboratories

Senior Scientist

Dr. Christopher Harrison, Sandia National Laboratories

Distinguished Member of the Technical Staff

Mission Challenges from Software

The widespread use of software that cannot be adequately characterized places our society at immeasurable risk and degrades our integrated deterrence.

Unintentional Supply Chain Scenario

Example: CrowdStrike Outage

Software Challenge: A new configuration file triggered an existing, undiscovered parsing bug in a widely deployed component.

Impact: The bug caused the system to crash, resulting in major disruption across multiple sectors including financial, health care, emergency services, airlines, and government.

Intentional Supply Chain Scenario

Example: SolarWinds Attack

Software Challenge: Malicious code was inserted in a software update of a popular IT administration platform.

Impact: the malicious update was distributed to over 18,000 customers across the globe, infecting key industry (e.g., Microsoft) and USG entities.

National Security Scenario

Example: DOD's F22 Crossing the Dateline

Software Challenge: Unexpected software behavior caused in-flight failure of navigation, fuel, and communications systems.

Impact: F22's aborted the mission and followed fully other functioning aircraft back to base.

Critical Infrastructure Scenario

Example: Salt Typhoon

Software Challenge: Gains initial access to its victim networks by targeting external-facing assets using known vulnerabilities.

Impact: Affecting major telecom companies and resulting in the theft of sensitive correspondence data, including metadata and call details.

Full Scope of the Problem

Examples are entirely notional, for illustration purposes only.

Full Scope of the Problem

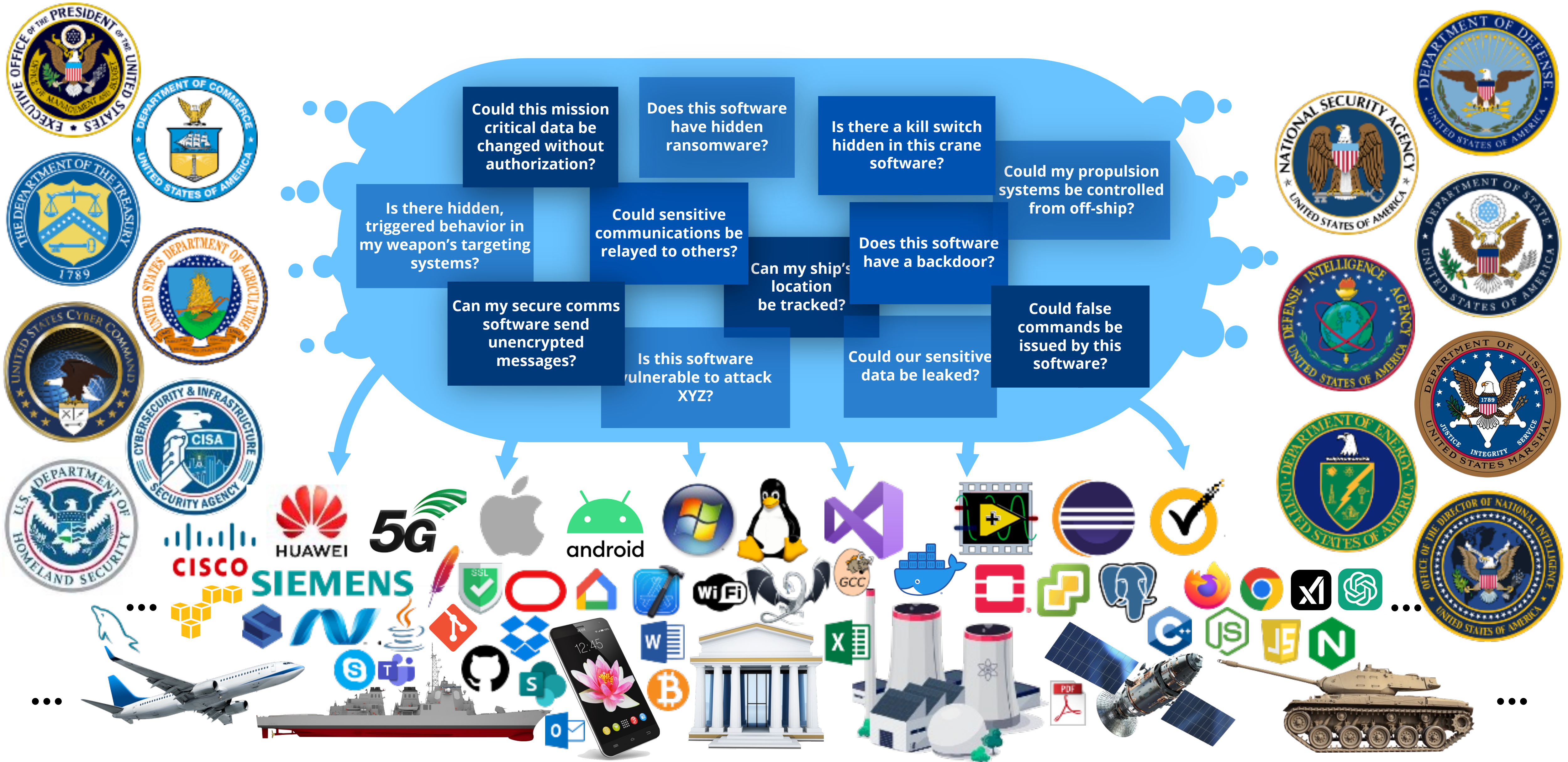
Examples are entirely notional, for illustration purposes only.

Full Scope of the Problem

EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
DEPARTMENT OF COMMERCE UNITED STATES OF AMERICA
THE DEPARTMENT OF THE TREASURY 1789
UNITED STATES DEPARTMENT OF AGRICULTURE
UNITED STATES CYBER COMMAND
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA
U.S. DEPARTMENT OF HOMELAND SECURITY
DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA
NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA
DEPARTMENT OF STATE UNITED STATES OF AMERICA
DEFENSE INTELLIGENCE AGENCY UNITED STATES OF AMERICA
DEPARTMENT OF JUSTICE 1789 JUSTICE INTEGRITY SERVICE UNITED STATES MARSHAL
DEPARTMENT OF ENERGY UNITED STATES OF AMERICA
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE UNITED STATES OF AMERICA
CISCO
HUAWEI
5G
android
SIEMENS
SSL
Wi Fi
GCC
W
X
S
T
O
PDF
12:45
...
...
...
...

Examples are entirely notional, for illustration purposes only.

Full Scope of the Problem



Could this mission critical data be changed without authorization?

Does this software have hidden ransomware?

Is there a kill switch hidden in this crane software?

Could my propulsion systems be controlled from off-ship?

Is there hidden, triggered behavior in my weapon's targeting systems?

Could sensitive communications be relayed to others?

Can my ship's location be tracked?

Does this software have a backdoor?

Can my secure comms software send unencrypted messages?

Is this software vulnerable to attack XYZ?

Could our sensitive data be leaked?

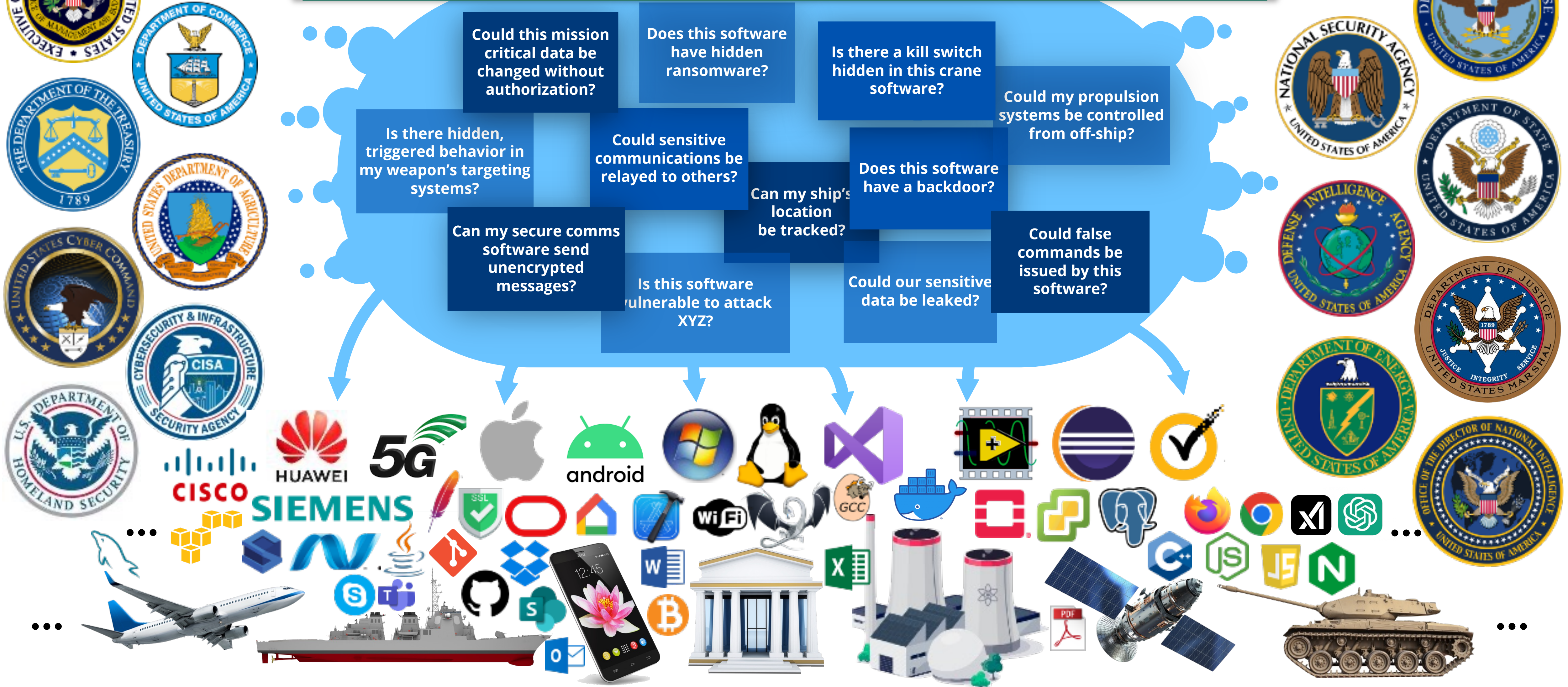
Could false commands be issued by this software?

SUNS
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
DEPARTMENT OF COMMERCE
THE DEPARTMENT OF THE TREASURY 1789
UNITED STATES DEPARTMENT OF AGRICULTURE
UNITED STATES CYBER COMMAND
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
U.S. DEPARTMENT OF HOMELAND SECURITY
DEPARTMENT OF DEFENSE
NATIONAL SECURITY AGENCY
DEPARTMENT OF STATE
DEFENSE INTELLIGENCE AGENCY
DEPARTMENT OF JUSTICE
UNITED STATES MARSHAL
DEPARTMENT OF ENERGY
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
CISCO
HUAWEI
5G
android
SIEMENS
Wi Fi
GCC
...
...
...
...

Examples are entirely notional, for illustration purposes only.

Full Scope of the Problem

Ideally, mission owners would be able to routinely analyze any mission critical software to answer any mission question.



Could this mission critical data be changed without authorization?

Does this software have hidden ransomware?

Is there a kill switch hidden in this crane software?

Could my propulsion systems be controlled from off-ship?

Is there hidden, triggered behavior in my weapon's targeting systems?

Could sensitive communications be relayed to others?

Does this software have a backdoor?

Can my ship's location be tracked?

Can my secure comms software send unencrypted messages?

Could false commands be issued by this software?

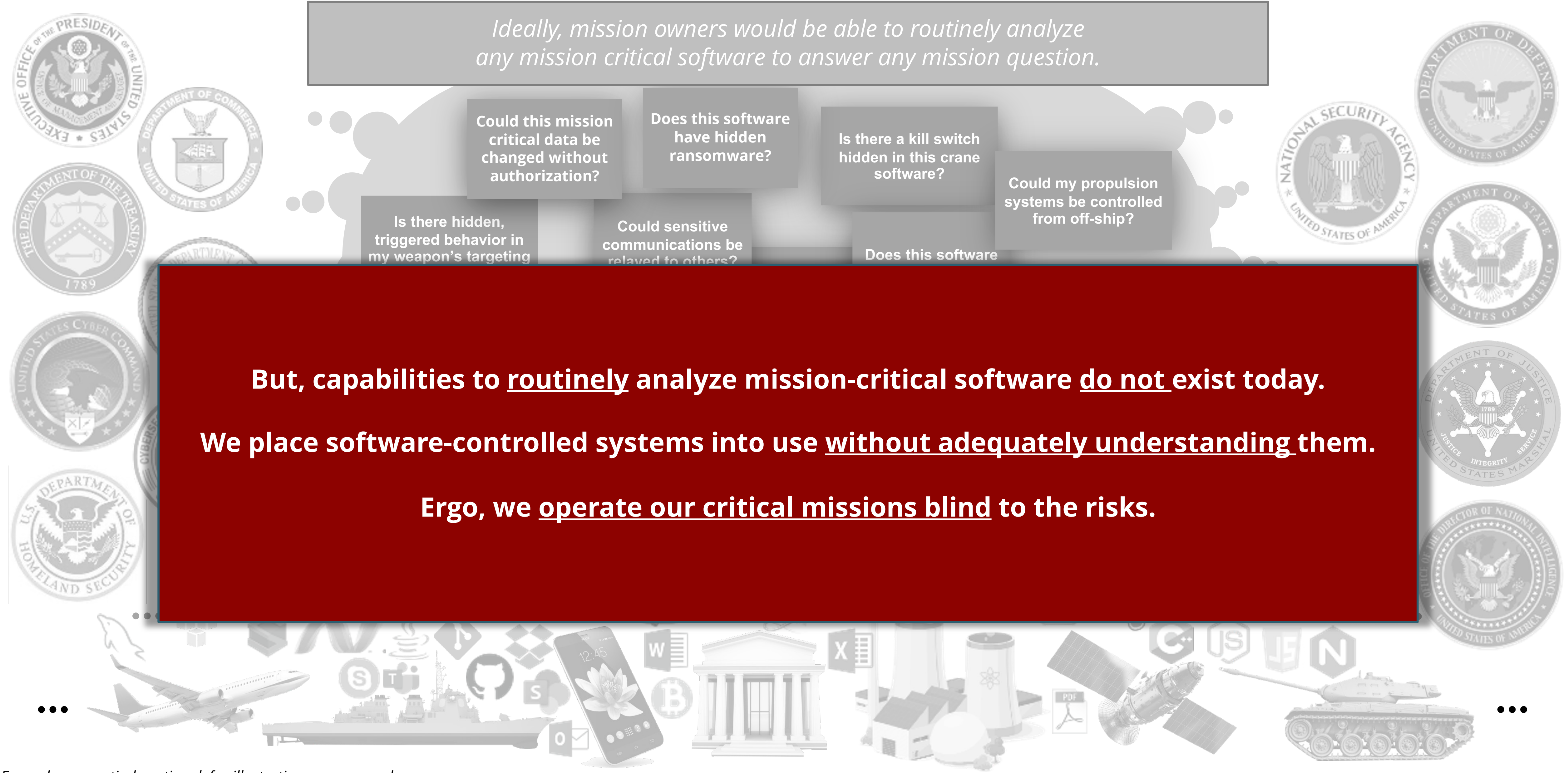
Is this software vulnerable to attack XYZ?

Could our sensitive data be leaked?

Examples are entirely notional, for illustration purposes only.

Full Scope of the Problem

Ideally, mission owners would be able to routinely analyze any mission critical software to answer any mission question.


Could this mission critical data be changed without authorization?
Does this software have hidden ransomware?
Is there a kill switch hidden in this crane software?
Could my propulsion systems be controlled from off-ship?
Is there hidden, triggered behavior in my weapon's targeting
Could sensitive communications be relayed to others?
Does this software

But, capabilities to <u>routinely</u> analyze mission-critical software <u>do not</u> exist today.

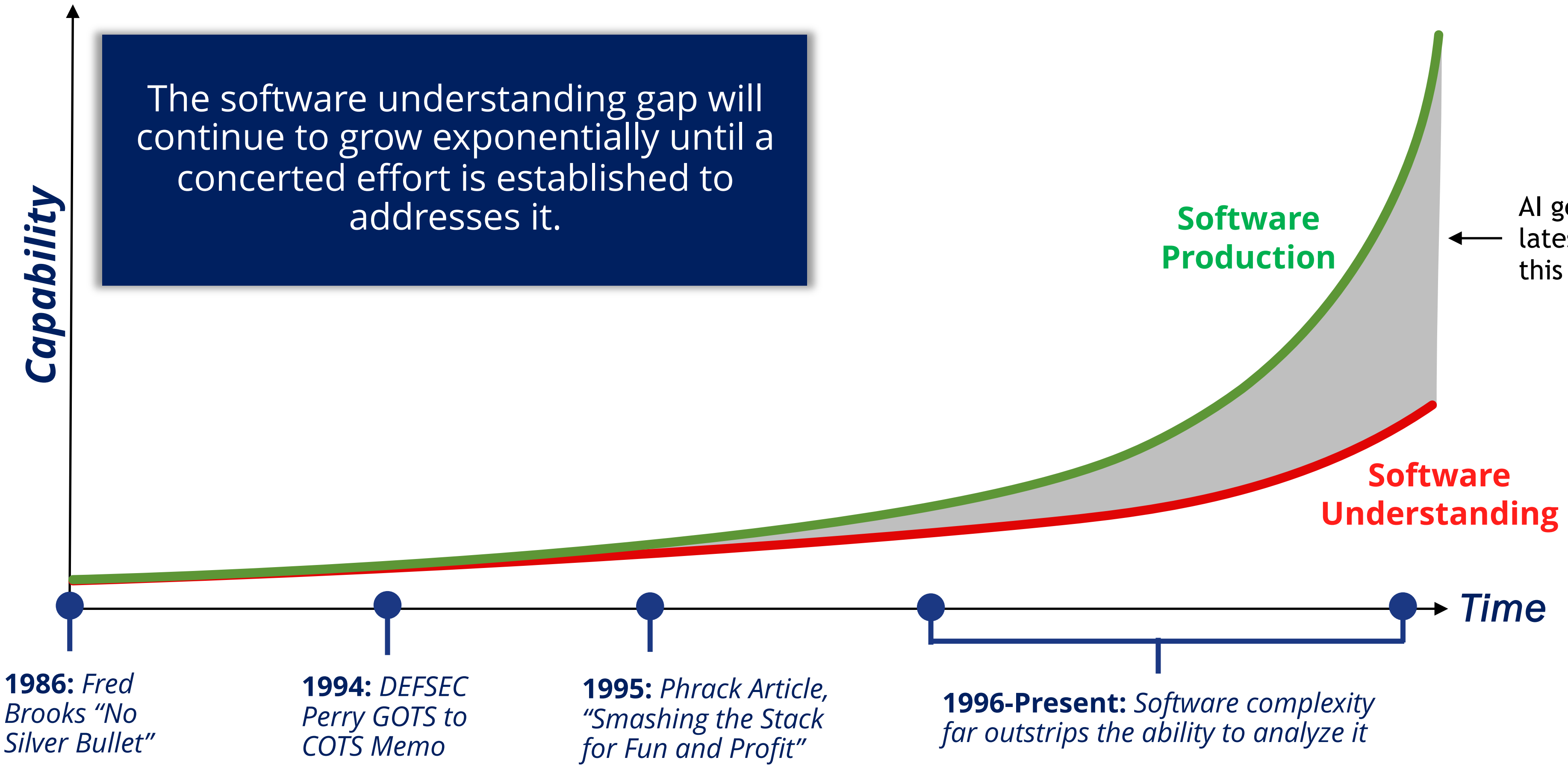
We place software-controlled systems into use <u>without adequately understanding</u> them.

Ergo, we <u>operate our critical missions blind</u> to the risks.

Examples are entirely notional, for illustration purposes only.

The Software Understanding Gap

Society's ability to produce software has far outstripped our ability to understand it – this gap drives the inscrutability of software behavior that imperils our missions.



The software understanding gap will continue to grow exponentially until a concerted effort is established to addresses it.

1986: *Fred Brooks "No Silver Bullet"*

1994: *DEFSEC Perry GOTS to COTS Memo*

1995: *Phrack Article, "Smashing the Stack for Fun and Profit"*

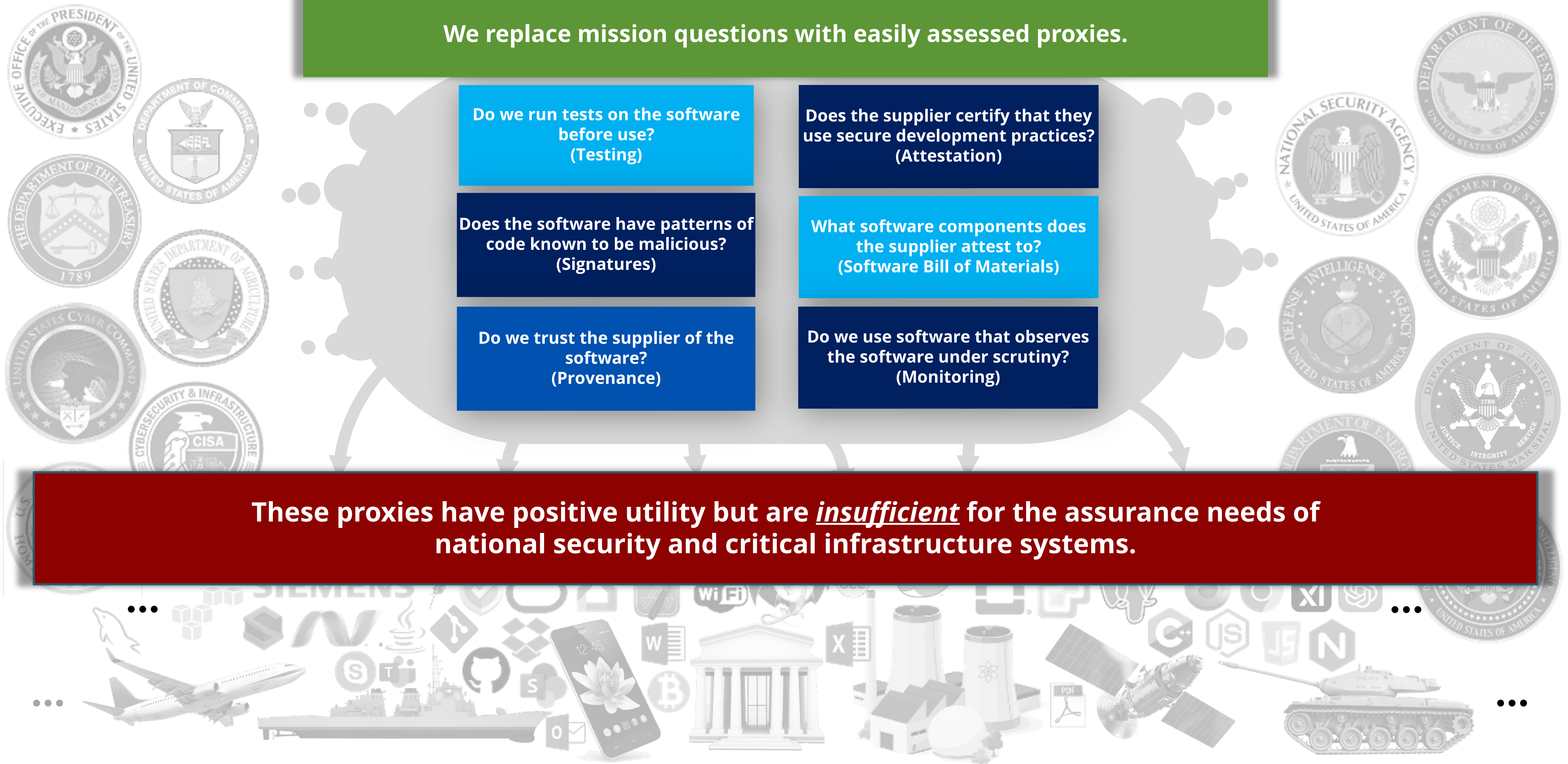
1996-Present: *Software complexity far outstrips the ability to analyze it*

AI generated code is the latest innovation driving this gap ever wider.

Examples are entirely notional, for illustration purposes only.

Full Scope of the Problem

We replace mission questions with easily assessed proxies.



Do we run tests on the software before use? (Testing)

Does the supplier certify that they use secure development practices? (Attestation)

Does the software have patterns of code known to be malicious? (Signatures)

What software components does the supplier attest to? (Software Bill of Materials)

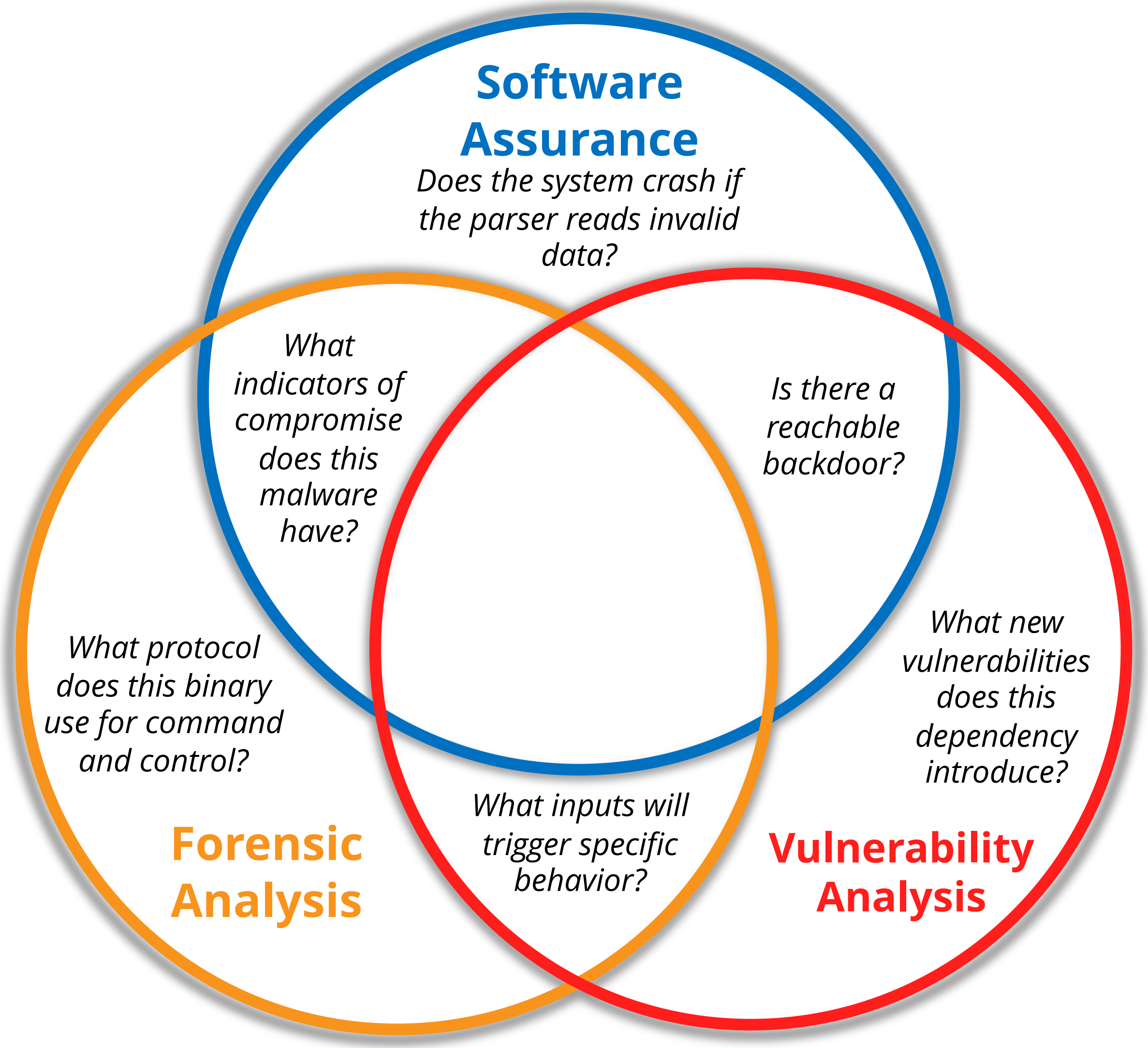
Do we trust the supplier of the software? (Provenance)

Do we use software that observes the software under scrutiny? (Monitoring)

These proxies have positive utility but are *insufficient* for the assurance needs of national security and critical infrastructure systems.

Examples are entirely notional, for illustration purposes only.

Software Understanding: *Taxonomy*



Software Assurance

Does the system crash if the parser reads invalid data?

What indicators of compromise does this malware have?

Is there a reachable backdoor?

What protocol does this binary use for command and control?

What new vulnerabilities does this dependency introduce?

What inputs will trigger specific behavior?

Forensic Analysis

Vulnerability Analysis

Software Understanding: *Taxonomy*

Malware Analysis

Network and Host Forensics

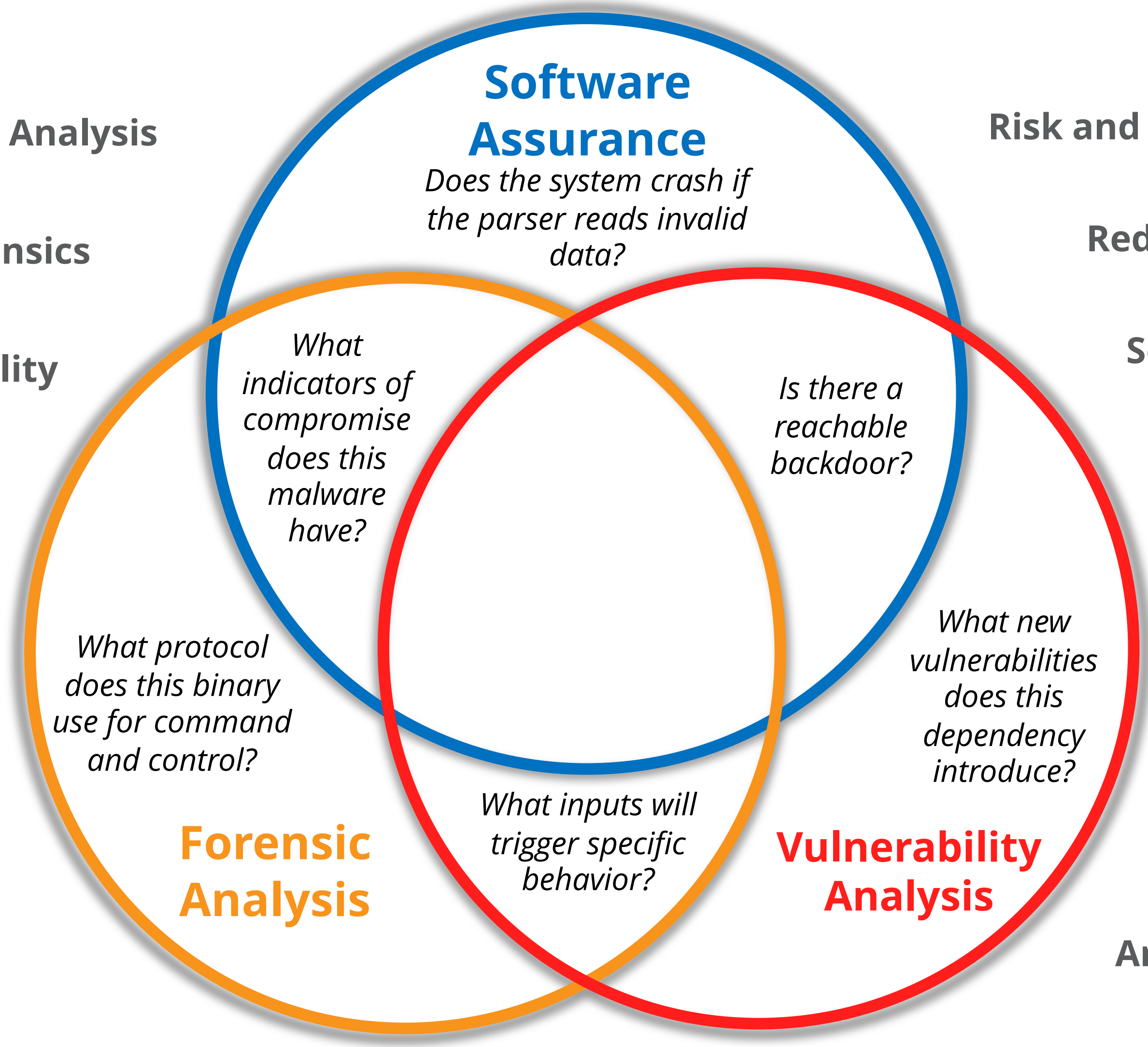
Software Dependability

Reverse Engineering

Log Analysis

Indicator Extraction

Cloud Telemetry Analysis


Software Assurance
Does the system crash if the parser reads invalid data?
What indicators of compromise does this malware have?
Is there a reachable backdoor?
What protocol does this binary use for command and control?
What new vulnerabilities does this dependency introduce?
What inputs will trigger specific behavior?
Forensic Analysis
Vulnerability Analysis

Risk and Vulnerability Assessment

Red Teaming

Secure Development Guidance

Remote Pen Testing

Vulnerability Scanning

Software Acquisition Guidance

Critical Product Evaluation

And More…

Software Understanding: *Taxonomy*

All these activities share a common need to reason about software—"software understanding."

Malware Analysis

Network and Host Forensics

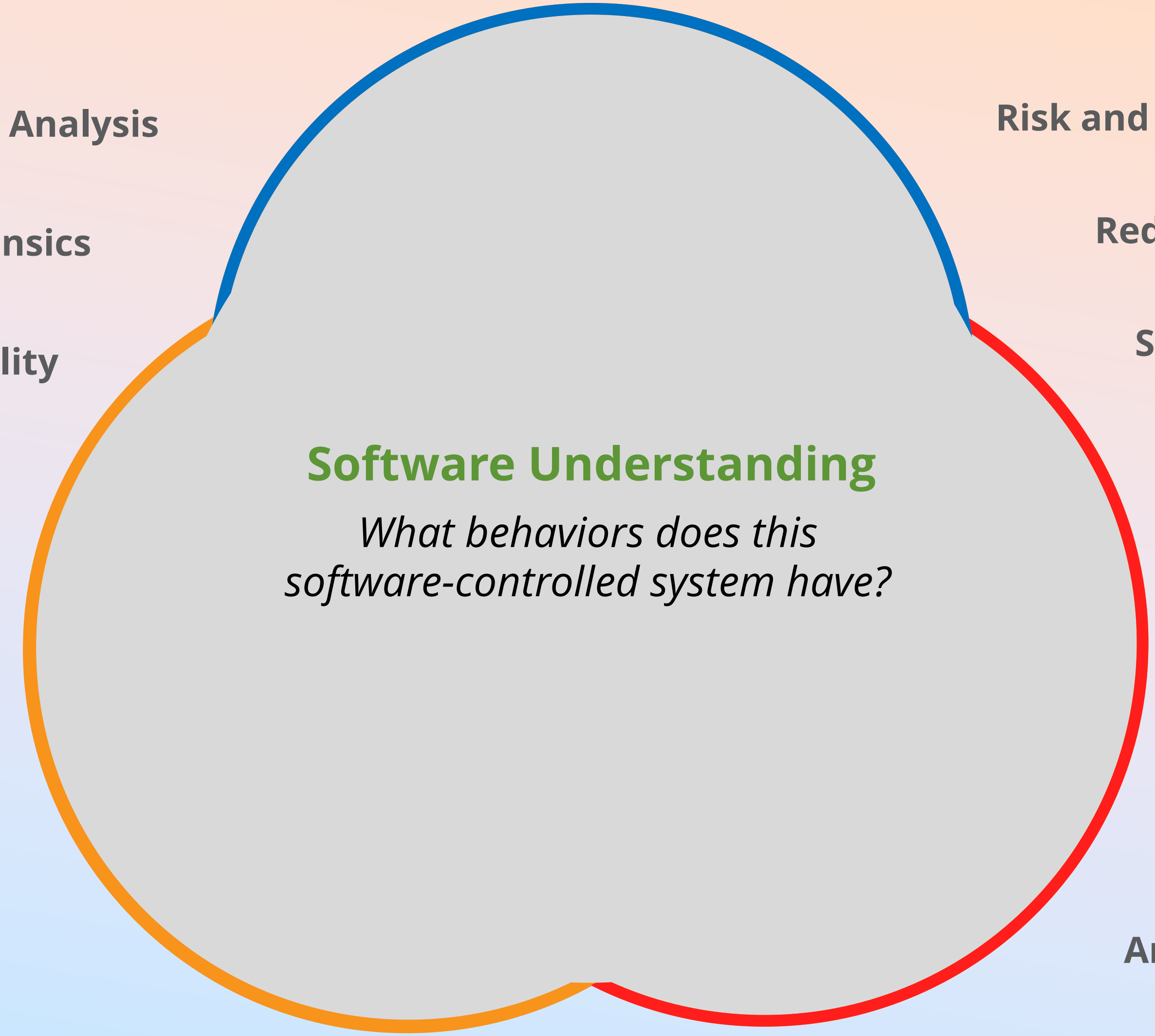
Software Dependability

Reverse Engineering

Log Analysis

Indicator Extraction

Cloud Telemetry Analysis



Software Understanding

What behaviors does this software-controlled system have?

Risk and Vulnerability Assessment

Red Teaming

Secure Development Guidance

Remote Pen Testing

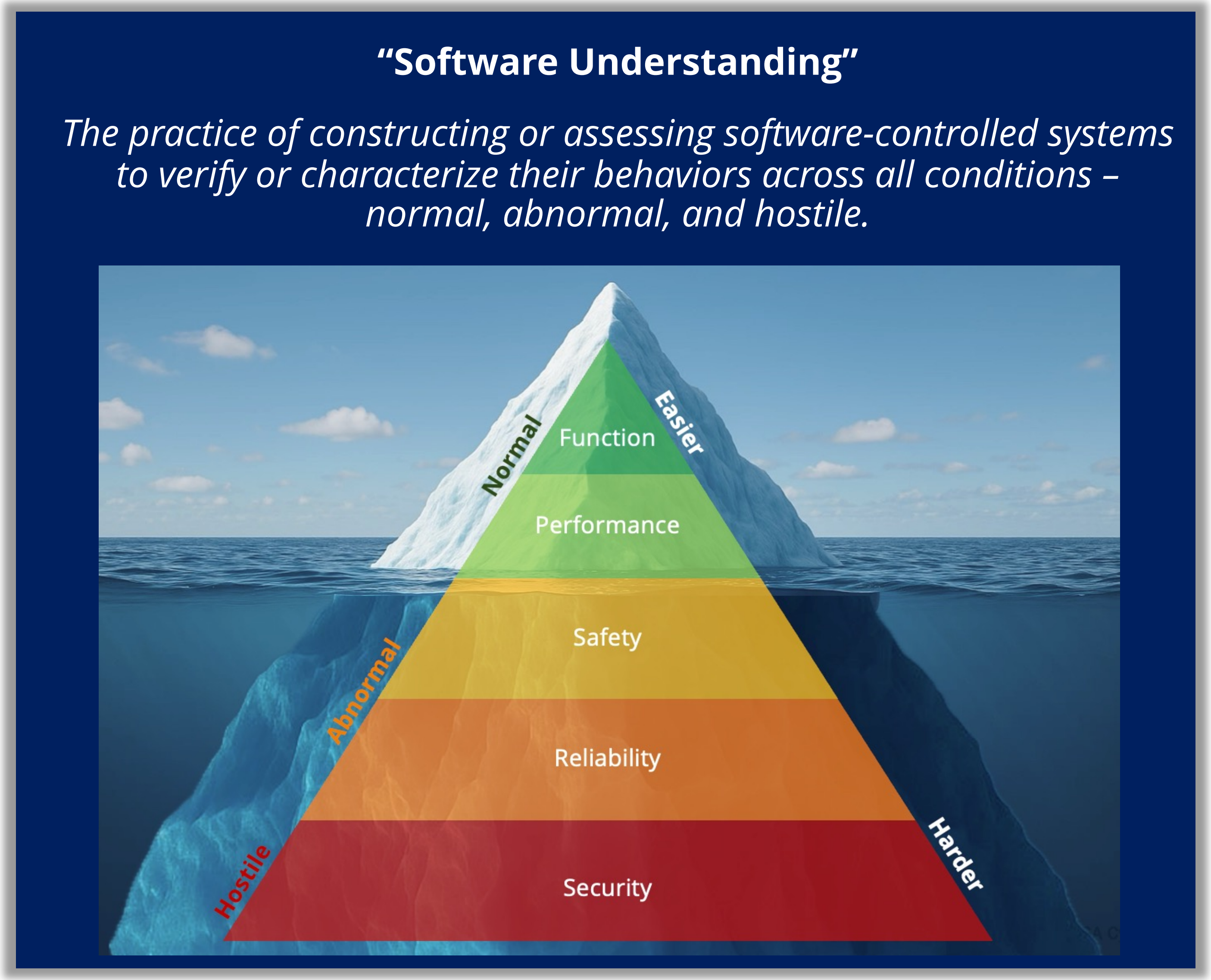
Vulnerability Scanning

Software Acquisition Guidance

Critical Product Evaluation

And More...

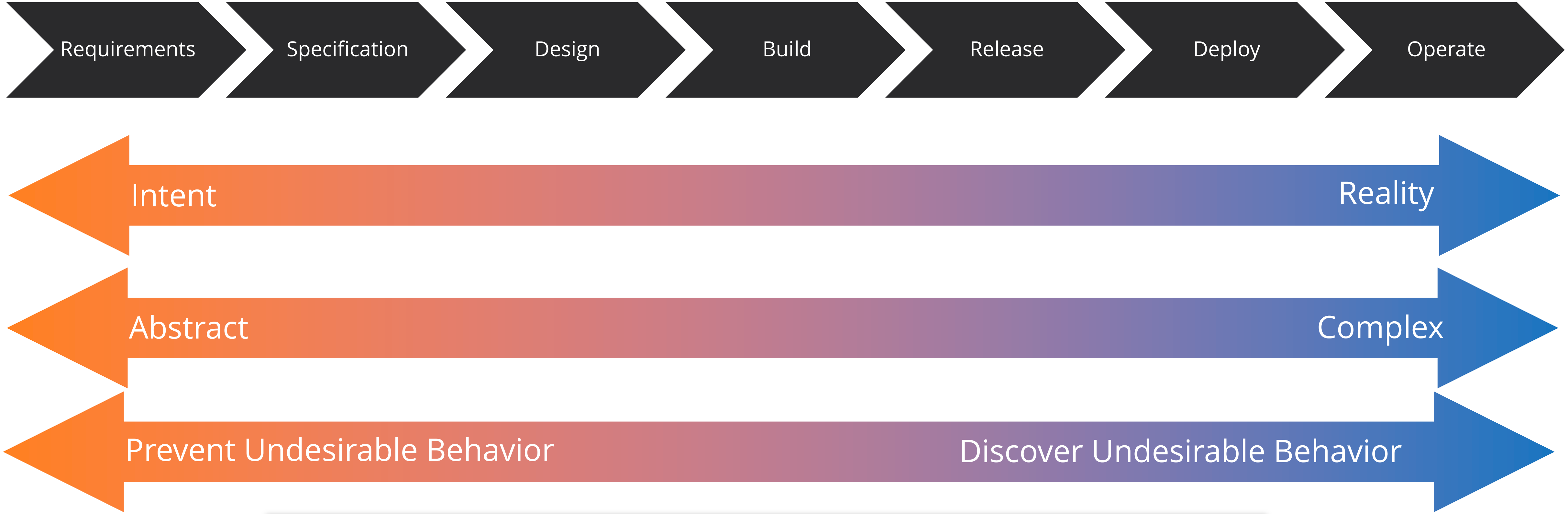
Software Understanding: *Definition*



“Software Understanding”

The practice of constructing or assessing software-controlled systems to verify or characterize their behaviors across all conditions – normal, abnormal, and hostile.

Software Understanding: *Decomposed*



Requirements

Specification

Design

Build

Release

Deploy

Operate

Intent

Reality

Abstract

Complex

Prevent Undesirable Behavior

Discover Undesirable Behavior

Forward Understanding

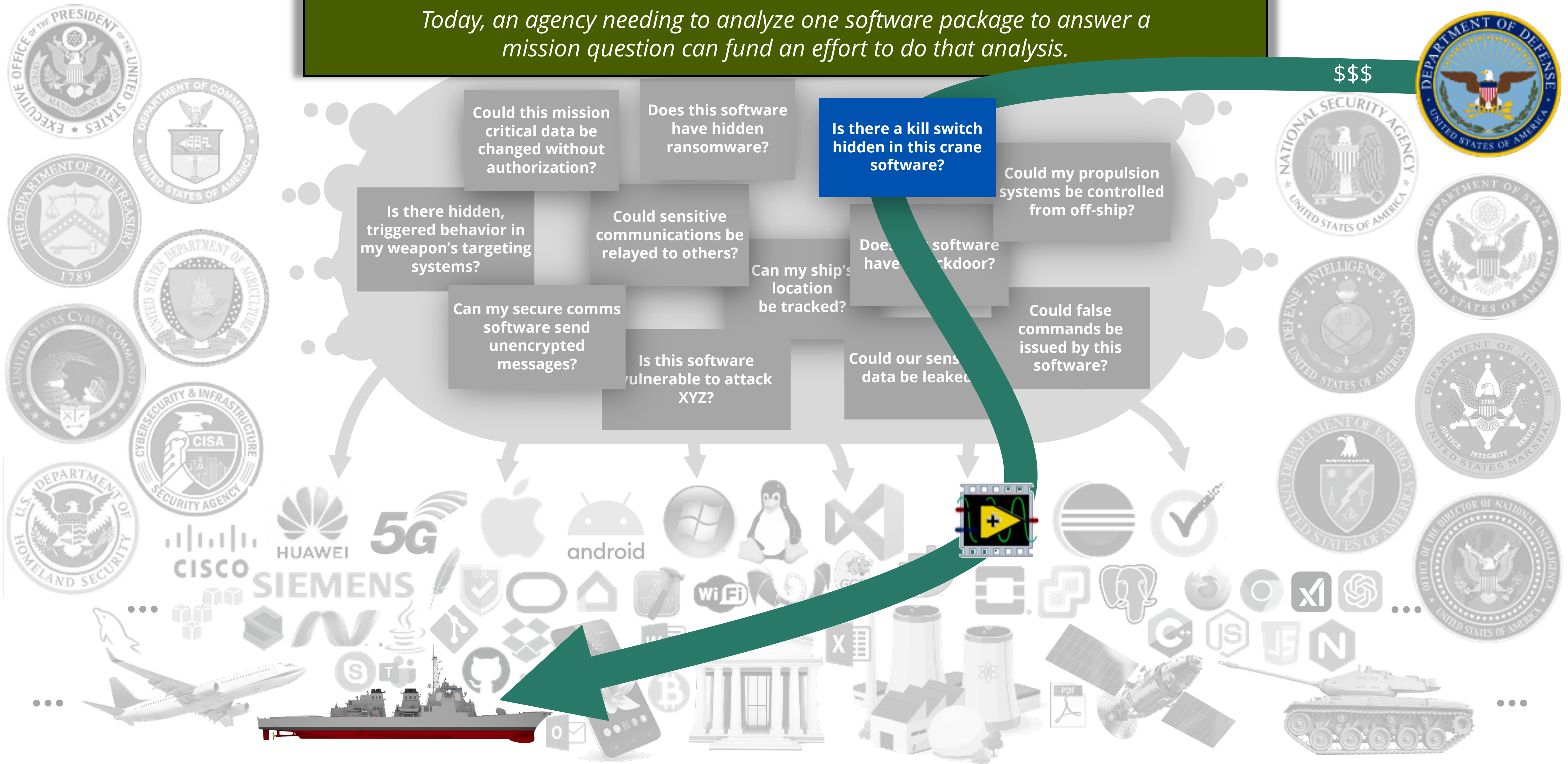
The practice of *constructing* of software-controlled systems to *verify* its behaviors.

Reverse Understanding

The practice of *assessing* of software-controlled systems to *characterize* its behaviors.

Full Scope of the Problem

Today, an agency needing to analyze one software package to answer a mission question can fund an effort to do that analysis.



Could this mission critical data be changed without authorization?

Does this software have hidden ransomware?

Is there a kill switch hidden in this crane software?

Could my propulsion systems be controlled from off-ship?

Is there hidden, triggered behavior in my weapon's targeting systems?

Could sensitive communications be relayed to others?

Can my ship's location be tracked?

Does software have ckdoor?

Can my secure comms software send unencrypted messages?

Is this software vulnerable to attack XYZ?

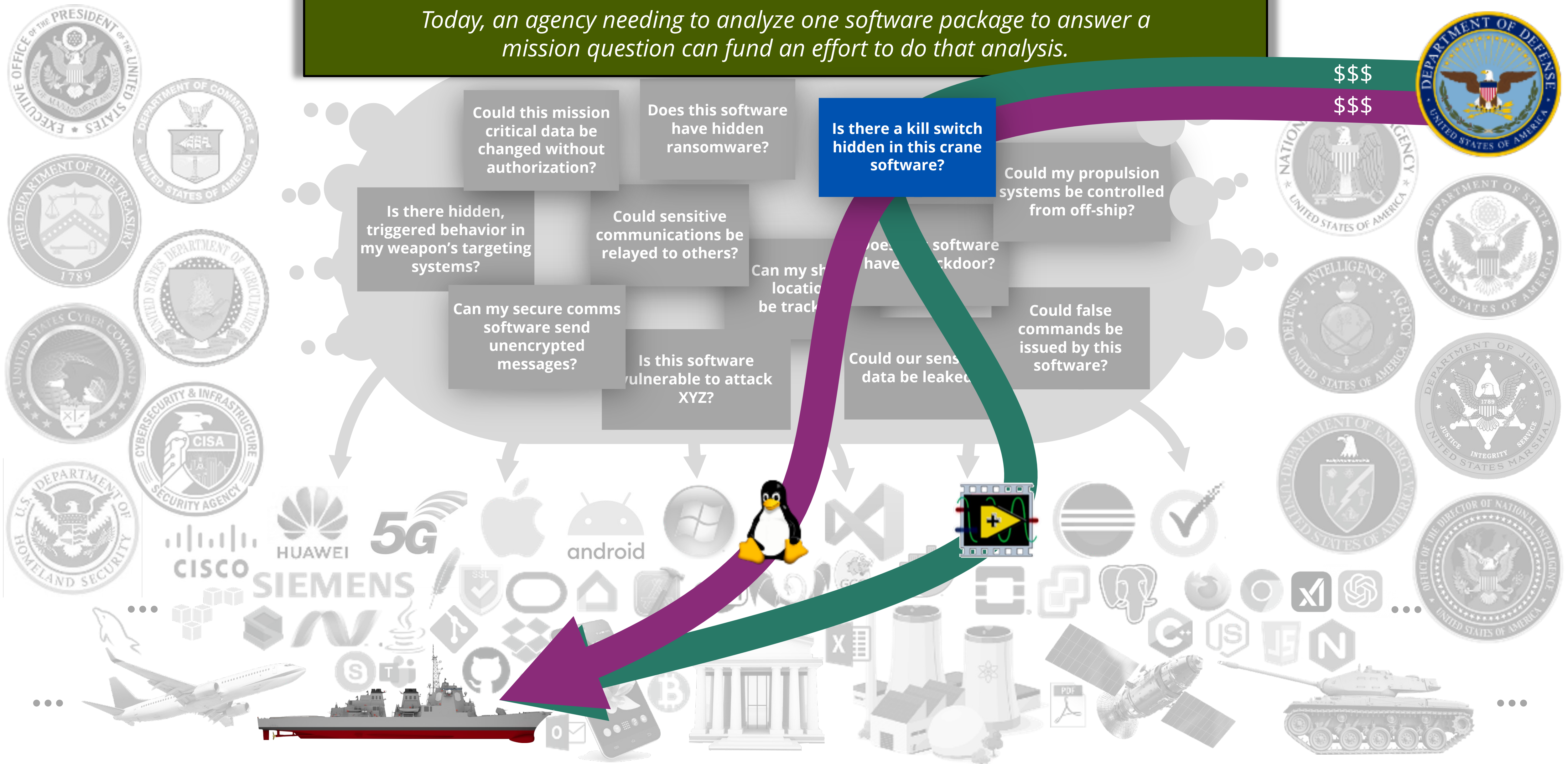
Could our sens data be leaked

Could false commands be issued by this software?

Examples are entirely notional, for illustration purposes only.

Full Scope of the Problem

Today, an agency needing to analyze one software package to answer a mission question can fund an effort to do that analysis.



Could this mission critical data be changed without authorization?

Does this software have hidden ransomware?

Is there a kill switch hidden in this crane software?

Could my propulsion systems be controlled from off-ship?

Is there hidden, triggered behavior in my weapon's targeting systems?

Could sensitive communications be relayed to others?

Can my sh locatio be track

oes software have ckdoor?

Can my secure comms software send unencrypted messages?

Is this software vulnerable to attack XYZ?

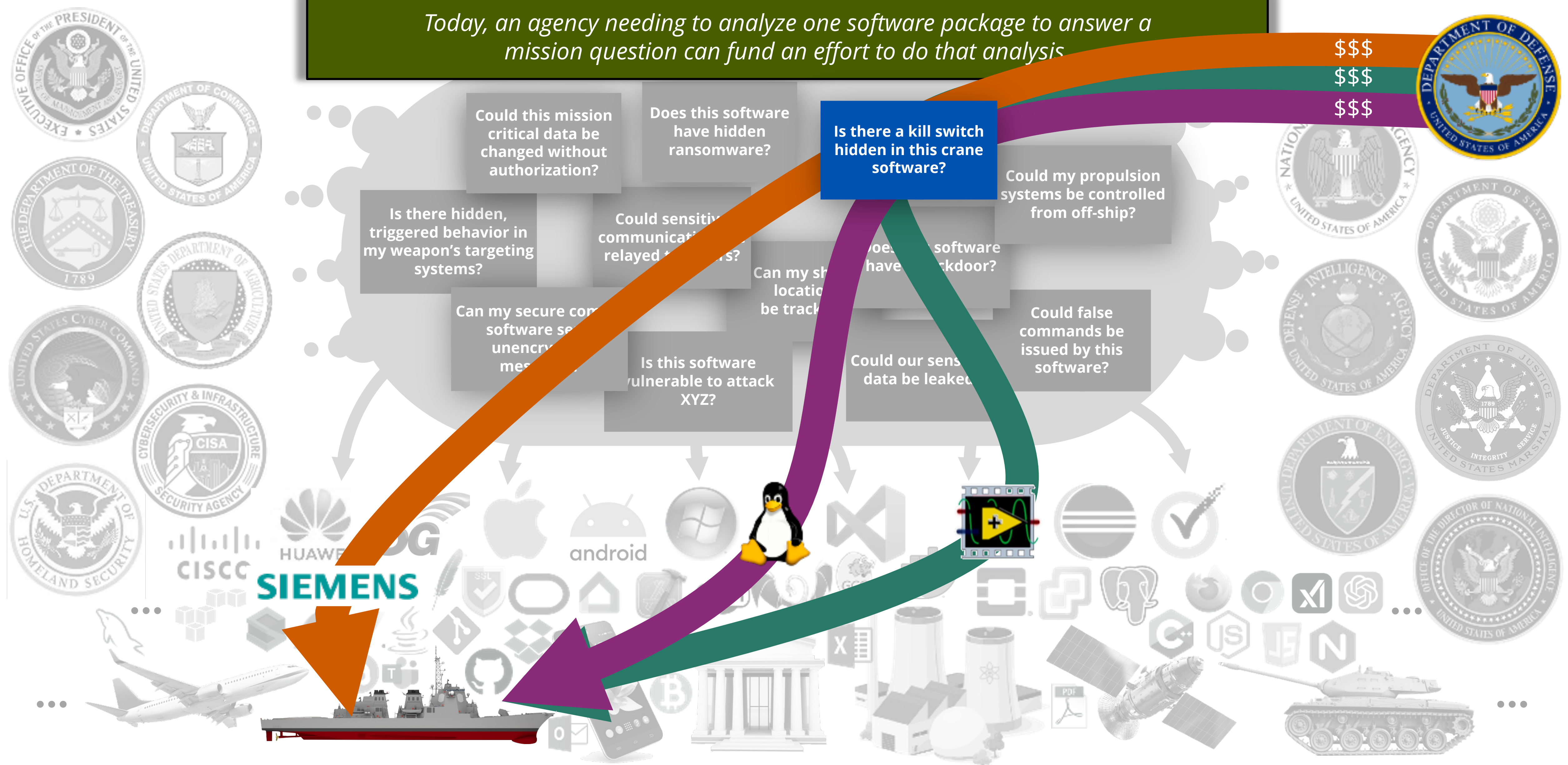
Could our sens data be leaked

Could false commands be issued by this software?

Examples are entirely notional, for illustration purposes only.

Full Scope of the Problem

Today, an agency needing to analyze one software package to answer a mission question can fund an effort to do that analysis



Could this mission critical data be changed without authorization?

Does this software have hidden ransomware?

Is there a kill switch hidden in this crane software?

Could my propulsion systems be controlled from off-ship?

Is there hidden, triggered behavior in my weapon's targeting systems?

Could sensitiv communicati relayed t s?

Can my sh locatio be track

oes software have kdoor?

Can my secure com software se unencry mes

Is this software vulnerable to attack XYZ?

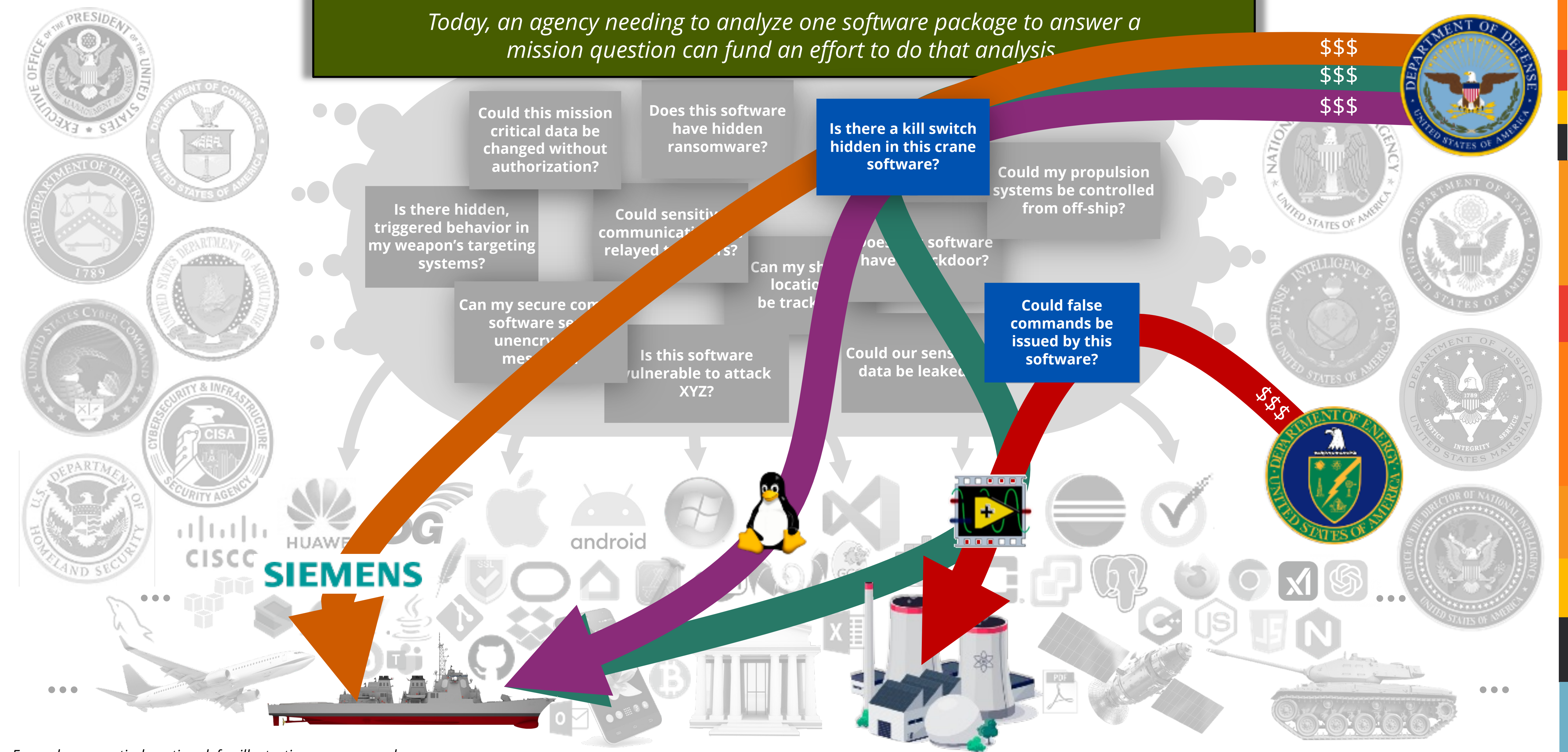
Could our sens data be leake

Could false commands be issued by this software?

Examples are entirely notional, for illustration purposes only.

Full Scope of the Problem

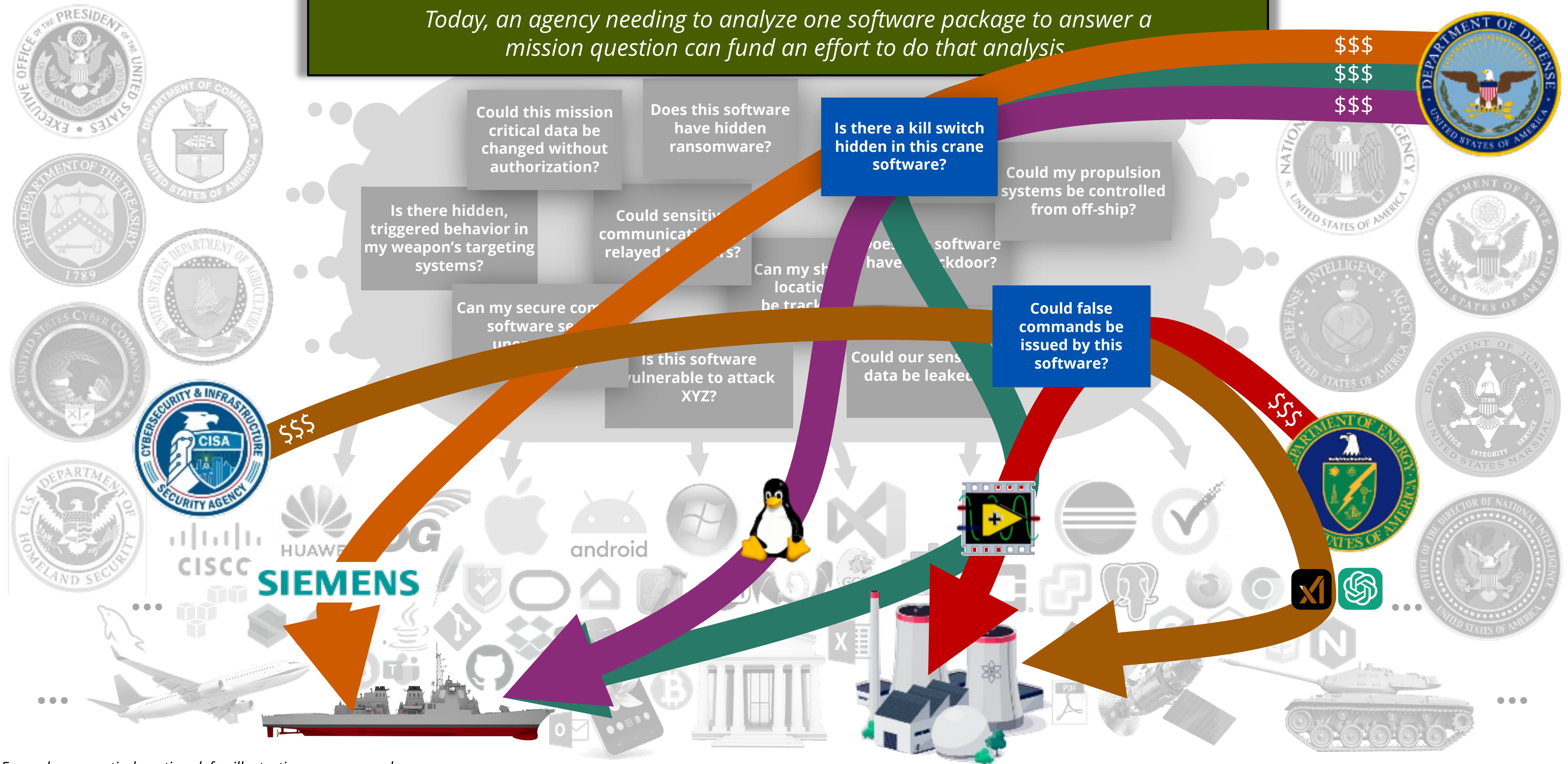
Today, an agency needing to analyze one software package to answer a mission question can fund an effort to do that analysis


SUNS
$$$
$$$
$$$
Could this mission critical data be changed without authorization?
Does this software have hidden ransomware?
Is there a kill switch hidden in this crane software?
Is there hidden, triggered behavior in my weapon's targeting systems?
Could sensitiv communicati relayed t s?
Could my propulsion systems be controlled from off-ship?
Can my sh locatio be track
oes software have ckdoor?
Can my secure com software se unencry mes
Is this software ulnerable to attack XYZ?
Could our sens data be leake
Could false commands be issued by this software?
$$$
HUAWE
5G
CISCO
SIEMENS
android

Examples are entirely notional, for illustration purposes only.

Full Scope of the Problem

Today, an agency needing to analyze one software package to answer a mission question can fund an effort to do that analysis



Could this mission critical data be changed without authorization?

Does this software have hidden ransomware?

Is there a kill switch hidden in this crane software?

Could my propulsion systems be controlled from off-ship?

Is there hidden, triggered behavior in my weapon's targeting systems?

Could sensitiv communicati relayed t s?

Can my sh locatio be track

oes software have ckdoor?

Can my secure com software se unc

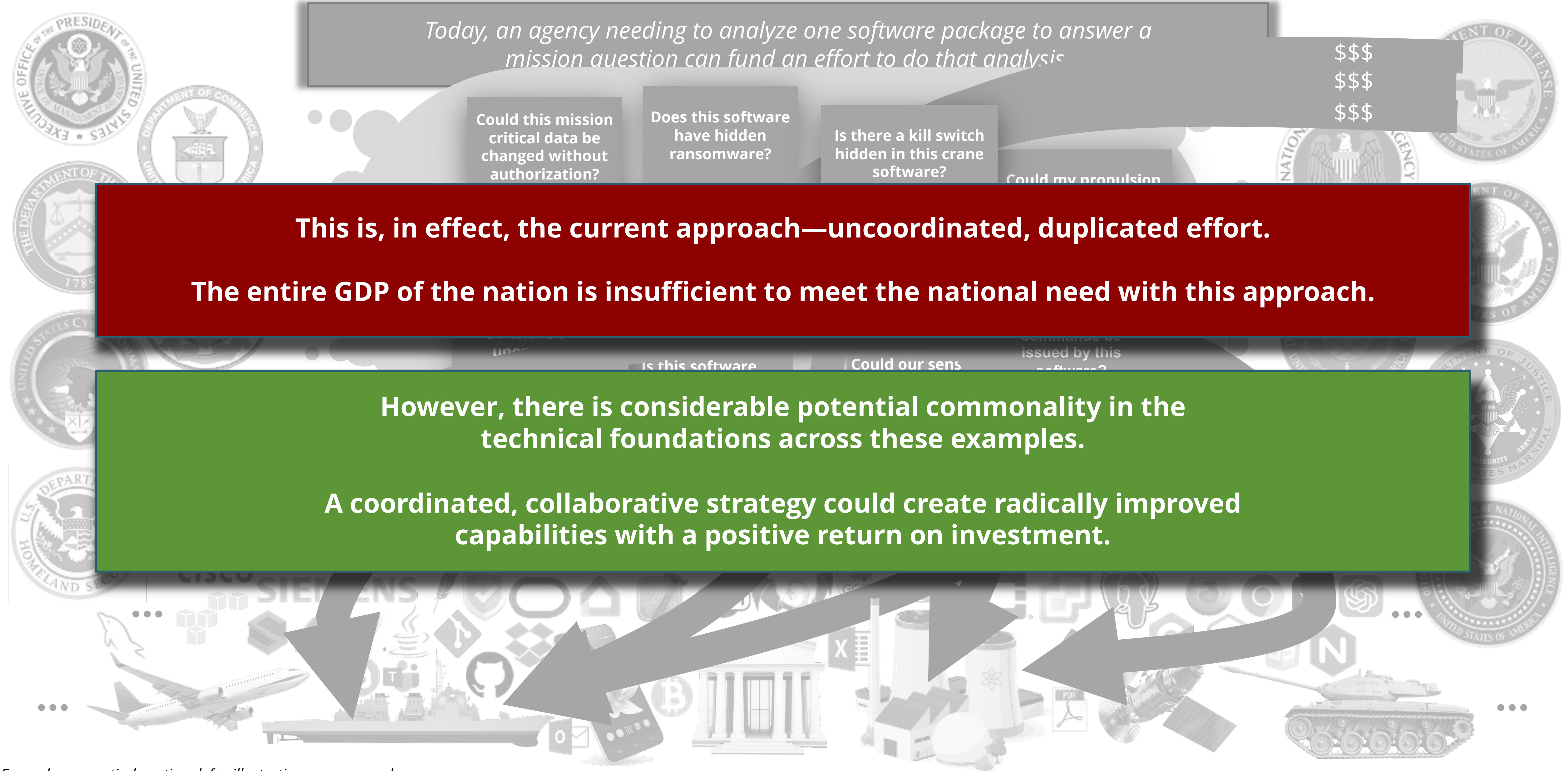
Is this software vulnerable to attack XYZ?

Could our sens data be leake

Could false commands be issued by this software?

Examples are entirely notional, for illustration purposes only.

Technical Opportunity



Today, an agency needing to analyze one software package to answer a mission question can fund an effort to do that analysis

$$$
$$$
$$$
Could this mission critical data be changed without authorization?
Does this software have hidden ransomware?
Is there a kill switch hidden in this crane software?
Could my propulsion
issued by this
Is this software
Could our sens
CISCO
SIEMENS
•••
•••
•••
•••

This is, in effect, the current approach—uncoordinated, duplicated effort.

The entire GDP of the nation is insufficient to meet the national need with this approach.

However, there is considerable potential commonality in the technical foundations across these examples.

A coordinated, collaborative strategy could create radically improved capabilities with a positive return on investment.

Examples are entirely notional, for illustration purposes only.

SUNS History: *Overview*

The USG has been wrestling with software understanding challenges for decades. Recently, efforts have focused on defining challenges, needs, and opportunities.

SUNS Workshop
(March 2023)

SUNS Technical Exchange Meeting
(March 2024)

SUNSEC Founders Meeting
(July 2024)

SUNS RD&E Roadmap
(December 2024)

Closing the Software Understanding Gap
(January 2025)

Software Understanding for National Security – Partnership Forum
(March 2025)

The National Need for Software Understanding
(March 2025)

2023
2024
2025
SUNS
DARPA
Closing the Software Understanding Gap

Presents a technical research, development, and engineering roadmap to enable the U.S. government to achieve greater software understanding.

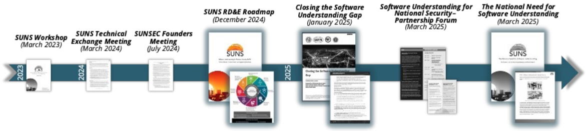
Defines a call to action for the U.S. government to take decisive and coordinated action to close the software understanding gap.

The forum served as the "launch event" for the "Closing the Software Understanding Gap" whitepaper.

Outlines the challenges of software understanding for NS&CI missions, discusses the shortcomings of traditional investment approaches, documents the outcomes of the SUNS 2023 Workshop and concludes with recommendations.

These documents are available at https://suns.sandia.gov/

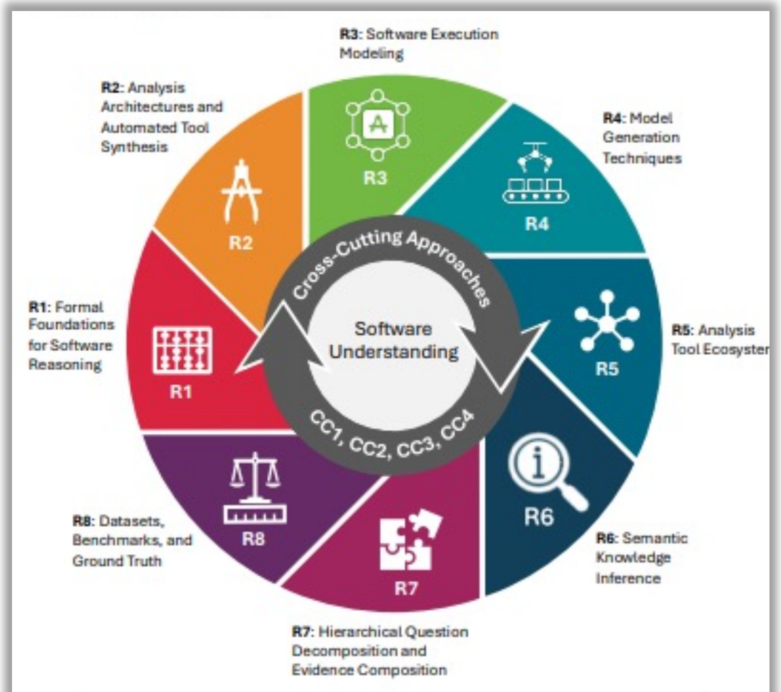
Technical RD&E Roadmap: *Overview*


2023
SUNS Workshop (March 2023)
2024
SUNS Technical Exchange Meeting (March 2024)
SUNSEC Founders Meeting (July 2024)
SUNS RD&E Roadmap (December 2024)
2025
Closing the Software Understanding Gap (January 2025)
Software Understanding for National Security– Partnership Forum (March 2025)
The National Need for Software Understanding (March 2025)

The RD&E roadmap outlines technical exploration options toward achieve a greater reverse understanding of software within NS&CI mission spaces.

Areas of Research in the Roadmap

1. Formal Foundations for Software Reasoning
2. Analysis Architectures and Automated Tool Synthesis
3. Software Execution Modeling
4. Model Generation Techniques
5. Analysis Tool Ecosystem
6. Semantic Knowledge Interference
7. Hierarchical Question Decomposition and Evidence Composition
8. Datasets, Benchmarks, and Ground Truth


R3: Software Execution Modeling
R2: Analysis Architectures and Automated Tool Synthesis
R4: Model Generation Techniques
R1: Formal Foundations for Software Reasoning
R5: Analysis Tool Ecosystem
R8: Datasets, Benchmarks, and Ground Truth
R6: Semantic Knowledge Inference
R7: Hierarchical Question Decomposition and Evidence Composition
R1
R2
R3
R4
R5
R6
R7
R8
Cross-Cutting Approaches
Software Understanding
CC1, CC2, CC3, CC4

Cross-Cutting Approaches

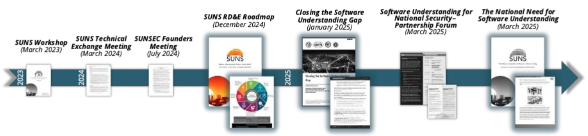
CC1: Dynamic and Static Analysis
CC2: Machine Learning, Artificial Intelligence, and Large Language Models
CC3: Human Factors and Human Studies
CC4: Design for Introspection and Debugging

Foundational Assumptions

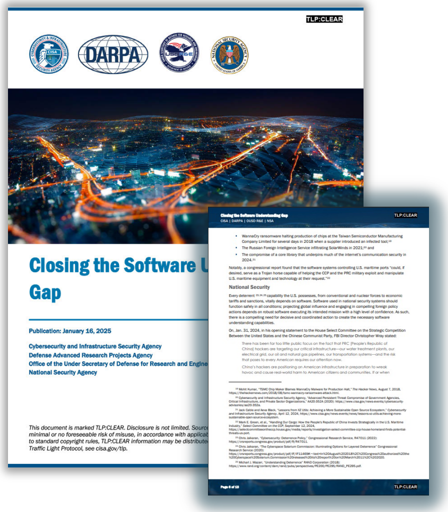
FA1: Mathematical Modeling
FA2: Composability

This document is available at https://suns.sandia.gov/

Closing the Software Understanding Gap


2023
SUNS Workshop
(March 2023)
2024
SUNS Technical Exchange Meeting
(March 2024)
SUNSEC Founders Meeting
(July 2024)
SUNS RD&E Roadmap
(December 2024)
2025
Closing the Software Understanding Gap
(January 2025)
Software Understanding for National Security–Partnership Forum
(March 2025)
The National Need for Software Understanding
(March 2025)

This report is a call to action for the US Government to take decisive and coordinated action to close the software understanding gap.



TLP:CLEAR

Closing the Software U

Gap

Publication: January 16, 2025

Cybersecurity and Infrastructure Security Agency
Defense Advanced Research Projects Agency
Office of the Under Secretary of Defense for Research and Engine
National Security Agency

This document is marked TLP:CLEAR. Disclosure is not limited. Source
minimal or no foreseeable risk of misuse, in accordance with applicab
to standard copyright rules, TLP:CLEAR information may be distribute
Traffic Light Protocol, see cisa.gov/tlp.

Closing the Software Understanding Gap
CISA | DARPA | OUSD R&E | NSA
TLP:CLEAR

- WannaCry ransomware halting production of chips at the Taiwan Semiconductor Manufacturing Company Limited for several days in 2018 when a supplier introduced an infected tool;[19]
- The Russian Foreign Intelligence Service infiltrating SolarWinds in 2021;[20] and
- The compromise of a core library that underpins much of the internet's communication security in 2024.[21]

Notably, a congressional report found that the software systems controlling U.S. maritime ports "could, if desired, serve as a Trojan horse capable of helping the CCP and the PRC military exploit and manipulate U.S. maritime equipment and technology at their request."[22]

National Security

Every deterrent [23,24,25] capability the U.S. possesses, from conventional and nuclear forces to economic tariffs and sanctions, vitally depends on software. Software used in national security systems should function safely in all conditions; projecting global influence and engaging in compelling foreign policy actions depends on robust software executing its intended mission with a high level of confidence. As such, there is a compelling need for decisive and coordinated action to create the necessary software understanding capabilities.

On, Jan. 31, 2024, in his opening statement to the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, FBI Director Christopher Wray stated:

> There has been far too little public focus on the fact that PRC [People's Republic of China] hackers are targeting our critical infrastructure—our water treatment plants, our electrical grid, our oil and natural gas pipelines, our transportation systems—and the risk that poses to every American requires our attention now.
>
> China's hackers are positioning on American infrastructure in preparation to wreak havoc and cause real-world harm to American citizens and communities. If or when

[19] Mohit Kumar, "TSMC Chip Maker Blames WannaCry Malware for Production Halt," *The Hacker News*, August 7, 2018, https://thehackernews.com/2018/08/tsmc-wannacry-ransomware-attack.html.

[20] Cybersecurity and Infrastructure Security Agency, "Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations," AA20-352A (2020): https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a.

[21] Jack Cable and Aeva Black, "Lessons from XZ Utils: Achieving a More Sustainable Open Source Ecosystem," *Cybersecurity and Infrastructure Security Agency*, April 12, 2024, https://www.cisa.gov/news-events/news/lessons-xz-utils-achieving-more-sustainable-open-source-ecosystem.

[22] Mark E. Green, et al., "Handling Our Cargo: How the People's Republic of China Invests Strategically in the U.S. Maritime Industry," *Select Committee on the CCP*, September 12, 2024, https://selectcommitteeontheccp.house.gov/media/reports/investigation-select-committee-ccp-house-homeland-finds-potential-threats-us-port.

[23] Chris Jaikaran, "Cybersecurity: Deterrence Policy," Congressional Research Service, R47011 (2022): https://crsreports.congress.gov/product/pdf/R/R47011.

[24] Chris Jaikaran, "The Cyberspace Solarium Commission: Illuminating Options for Layered Deterrence" Congressional Research Service (2020): https://crsreports.congress.gov/product/pdf/IF/IF11469#:~:text=In%20August%202018%2C%20Congress%20authorized%20the%20Cyberspace%20Solarium,Commission%20released%20its%20report%20on%20March%2011%2C%202020.

[25] Michael J. Mazarr, "Understanding Deterrence" RAND Corporation (2018): https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf.

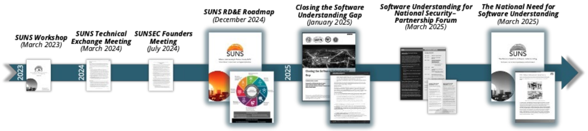
Page 6 of 13
TLP:CLEAR

Closing the Software Understanding Gap

Call to Action

1. **Policy Action:** Reconsider policy to accelerate the development and adoption of software understanding capabilities and cultivate software understanding as a critical national resource.
2. **Technology Procurement:** Reimagine acquisition of software to drive risk lower by empowering the U.S. government to foster and incentivize the widespread adoption of ever-advancing capabilities.
3. **Technical Solutions:** Establish coordinated foundational and applied R&D efforts to invest in common solutions that advance national capabilities more broadly and cost-effectively.

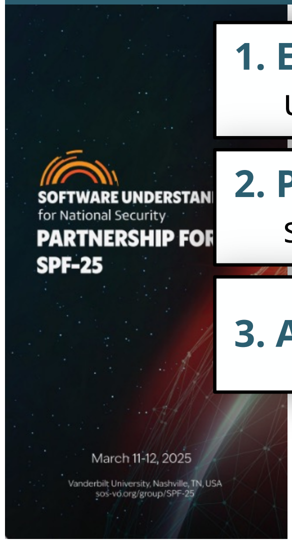
2025 SUNS Partnership Forum (SPF)


SUNS Workshop
(March 2023)
SUNS Technical Exchange Meeting
(March 2024)
SUNSEC Founders Meeting
(July 2024)
SUNS RD&E Roadmap
(December 2024)
Closing the Software Understanding Gap
(January 2025)
Software Understanding for National Security–Partnership Forum
(March 2025)
The National Need for Software Understanding
(March 2025)
2023
2024
2025

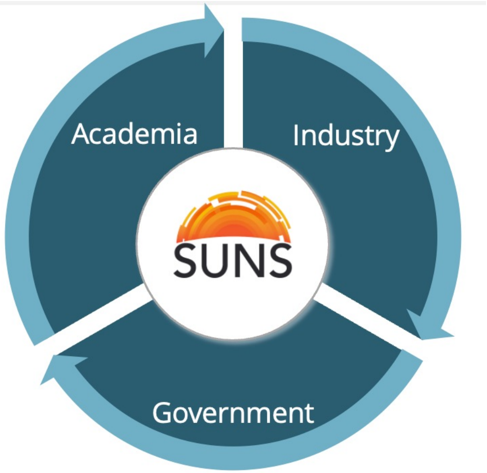
SUNS

The SUNS Partnership Forum 2025 (SPF-25) served as a launch event for the "Closing the Software Understanding Gap" report.

SPF-25 Goals



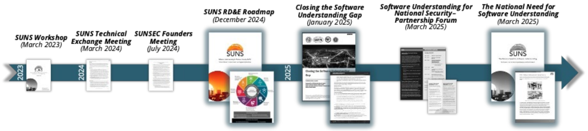
1. **Engagement:** Engage academia, industry, and government on the software understanding problem.
2. **Perspective:** Gather perspectives on the problem, challenges, and potential solutions.
3. **Action:** Identify actions that the SUNS partners can each take.



The event brought together the communities below to foster engagement, explore solutions, and promote collaboration in closing the software understanding gap.

VANDERBILT UNIVERSITY · DARPA · LOCKHEED MARTIN · galois · aws · Collins Aerospace · Qualcomm · Atalanta THERAPEUTICS · ASU · Sandia National Laboratories · INL Idaho National Laboratory · leidos · twosix TECHNOLOGIES · Microsoft · SRI International · National Cyber Security Centre a part of GCHQ · NSF · NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA

2025 SPF: *Structure*


SUNS Workshop
(March 2023)
SUNS Technical Exchange Meeting
(March 2024)
SUNSEC Founders Meeting
(July 2024)
SUNS RD&E Roadmap
(December 2024)
Closing the Software Understanding Gap
(January 2025)
Software Understanding for National Security–Partnership Forum
(March 2025)
The National Need for Software Understanding
(March 2025)
2023
2024
2025

SUNS

SPF-25 was structured to be a combination of keynotes, panels, and breakout group discussions to maximize interaction.

Breakout 1

The National Problem

Discussion Questions

- *What are your thoughts on the national need in software understanding as described?*
- *What gaps in the software understanding problem, are most important to prioritize?*

Breakout 2

The Non-Technical Solution Space

Discussion Questions

- *What prevents us from making progress toward adequately addressing the national software understanding problem?*
- *What investments are needed to address this problem adequately, including resources, types of resources, timeframe?*

Breakout 3

The Technical Solution Space

Discussion Questions

- *What technical domains need to be involved in developing the solutions?*
- *What age-old but under-funded techniques need a boost of investment? What underexplored novel techniques should be prioritized?*

Breakout 4

Next Steps for the Nation

Discussion Questions

- *Can the software understanding problem be addressed short of a national effort, and if so, how?*
- *Given the pervasiveness and seriousness of the problem, what type of national effort might be best suited to address this problem?*

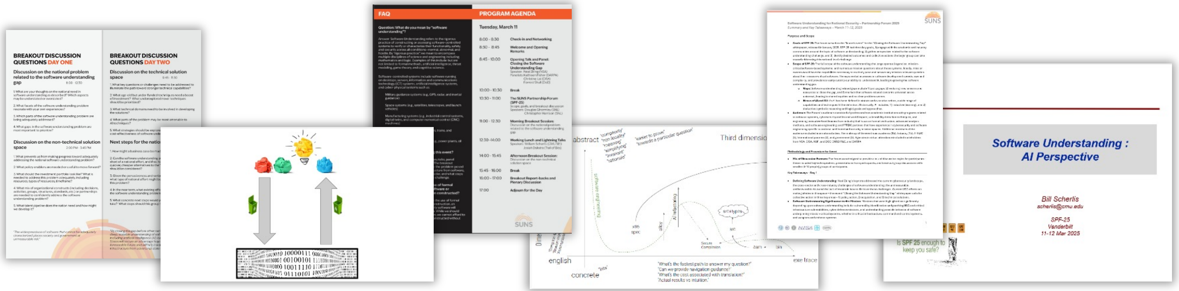
Each breakout session had 3 groups with a mix of industry, academia, and former government individuals.

2025 SPF: *Outcomes and Key Takeaways*

SPF outlined the significance of the software understanding challenge from academic, industry, and government viewpoint – while highlighting the needed next steps.

Key Takeaways

- **Agreement Across Academia and Industry:** Broad agreement on the national-level challenge and scope.
- **Software Understanding to Drive Solutions:** Broad agreement on Software Understanding as a powerful concept in elucidating the opportunity cost of the current approach and the commonality that could drive solutions.
- **Lack of National Level Efforts:** There was no alternative identified to a national level effort in software understanding.
- **Government Has A Key Role in Discussions:** The absence of the government during discussions was notably impactful, particularly in certain policy areas, such as acquisition.


BREAKOUT DISCUSSION QUESTIONS DAY ONE
BREAKOUT DISCUSSION QUESTIONS DAY TWO
FAQ
PROGRAM AGENDA
Tuesday, March 11
abstract
Third dimension
english
concrete
exe trace
Software Understanding : AI Perspective
Bill Scherlis
scherlis@cmu.edu
SPF-25
Vanderbilt
11-12 Mar 2025
Is SPF 25 enough to keep you safe?
SUNS

Proposed Next Steps

1. Engagement with DOD (OUSD R&E, A&S, DARPA) – in particular, multiple participants favored a new DARPA program focused on Software Understanding.
2. Producing and providing a Software Understanding technical packet to the Congressional Research Service.
3. Engagement with NITRD, the National Academies, CAE Symposium, HCSS, and other venues.
4. Engagement with the administration (ONCD, OSTP, OMB, NSC, etc.).

SUNS