ONR Information, Cyber, and Spectrum Superiority

Mathematics, Computer, and Information Sciences (MCIS) division

Secure and Resilient Systems Research at ONR

Trusted Computing Center of Excellence Summit

Dr. Ryan Craven
10 May 2024

ACCELERATING TO THE NAVY & MARINE CORPS AFTER NEXT

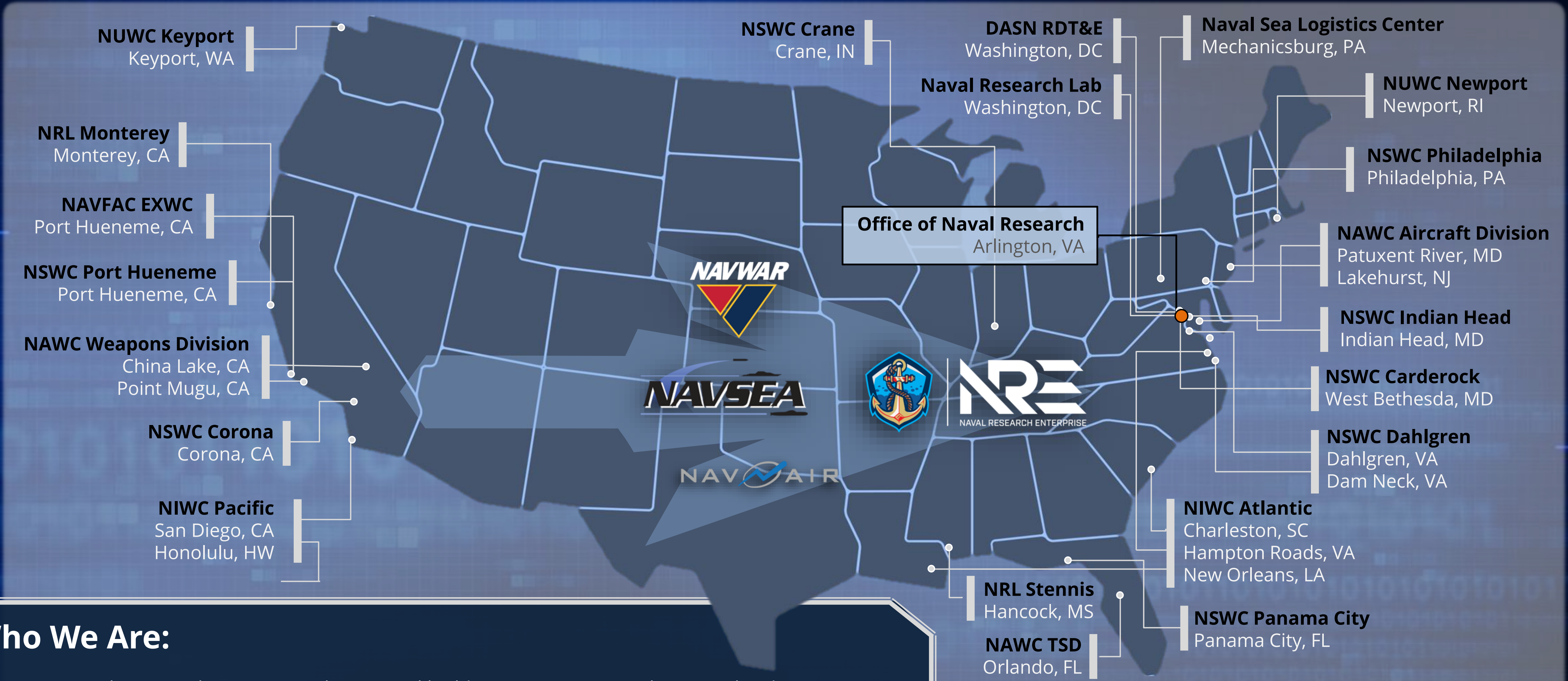
DISTRIBUTION STATEMENT A: Approved for public release.
Document Control Number (DCN): 0543-1789-24

The contents of this briefing are: **UNCLASSIFIED**

Hi! I’m a **Program Officer** at the **Office of Naval Research (ONR)**.

First a few quick slides of context…

The Naval R&D Establishment (NR&DE)



NUWC Keyport
Keyport, WA

NRL Monterey
Monterey, CA

NAVFAC EXWC
Port Hueneme, CA

NSWC Port Hueneme
Port Hueneme, CA

NAWC Weapons Division
China Lake, CA
Point Mugu, CA

NSWC Corona
Corona, CA

NIWC Pacific
San Diego, CA
Honolulu, HW

NSWC Crane
Crane, IN

DASN RDT&E
Washington, DC

Naval Research Lab
Washington, DC

Office of Naval Research
Arlington, VA

Naval Sea Logistics Center
Mechanicsburg, PA

NUWC Newport
Newport, RI

NSWC Philadelphia
Philadelphia, PA

NAWC Aircraft Division
Patuxent River, MD
Lakehurst, NJ

NSWC Indian Head
Indian Head, MD

NSWC Carderock
West Bethesda, MD

NSWC Dahlgren
Dahlgren, VA
Dam Neck, VA

NIWC Atlantic
Charleston, SC
Hampton Roads, VA
New Orleans, LA

NRL Stennis
Hancock, MS

NAWC TSD
Orlando, FL

NSWC Panama City
Panama City, FL

NAWC	Naval Air Warfare Center
NIWC	Naval Information Warfare Center
NSWC	Naval Surface Warfare Center
NUWC	Naval Undersea Warfare Center
EXWC	Engineering and Expeditionary Warfare Center

Who We Are:

- 20 commands across the NAVWAR/NAVAIR/NAVSEA Warfare Centers and the Naval Research Enterprise
- A diverse and highly educated workforce with 25,000 scientists, engineers, and technicians (and 2,000+ PhDs)
- We discover, develop, transition, and field technologically superior naval warfighting capabilities for the Department of Navy

NRE
NAVAL RESEARCH ENTERPRISE

The Headquarters Activity for Naval S&T

Established in 1946, ONR is headquartered in Arlington, VA. ONR partners with industry, academia, and government to coordinate and sponsor S&T for U.S. Navy and Marine Corps.

The Department of Navy's Corporate Laboratory

Founded in 1923, NRL is headquartered in Washington, DC with four field sites across the U.S.

Engage the International Community

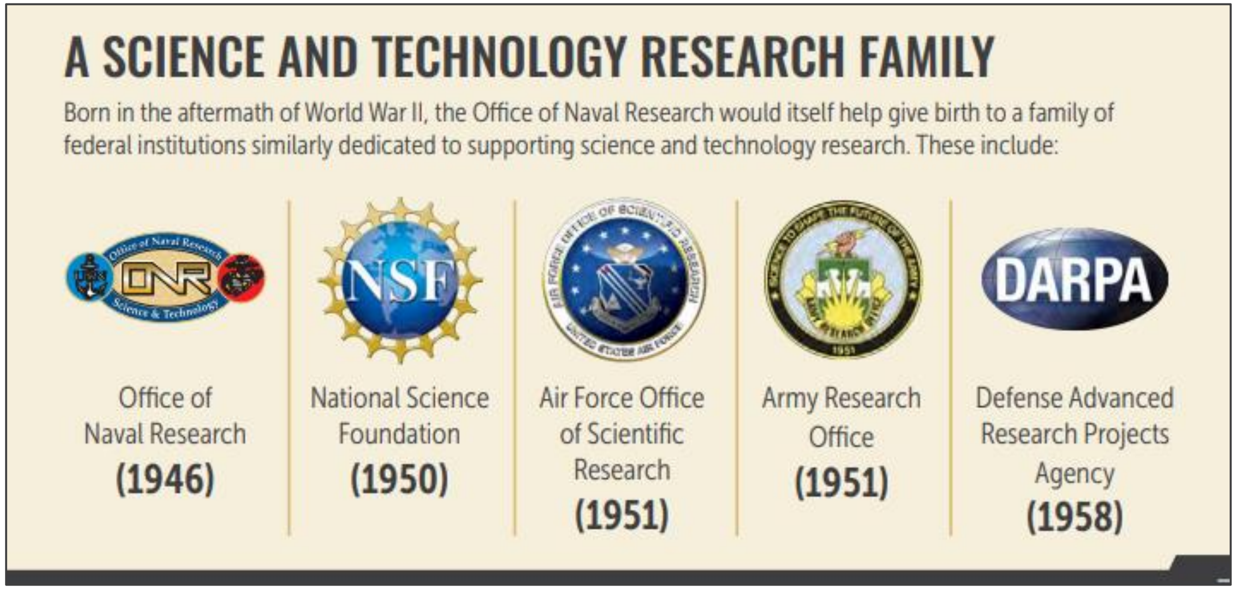
Connects the NRE with 1000+ partners in 58 countries.

Agility and Innovation Cell

https://www.nre.navy.mil/

About ONR

- First of the Post-WW2 wave of new federal agencies to coordinate the efforts of civilian scientists and inventors for the sake of national defense
  - Long and productive history of engaging academic community
  - ONR performers have been awarded over 70 Nobel Prizes
- 6.1 Basic Research, 6.2 Applied Research, and 6.3 Advanced Tech Development are all under one roof
  - Allows us to bridge the gap between cutting edge scientific research and fieldable prototypes



A SCIENCE AND TECHNOLOGY RESEARCH FAMILY

Born in the aftermath of World War II, the Office of Naval Research would itself help give birth to a family of federal institutions similarly dedicated to supporting science and technology research. These include:

Office of Naval Research (1946)

National Science Foundation (1950)

Air Force Office of Scientific Research (1951)

Army Research Office (1951)

Defense Advanced Research Projects Agency (1958)

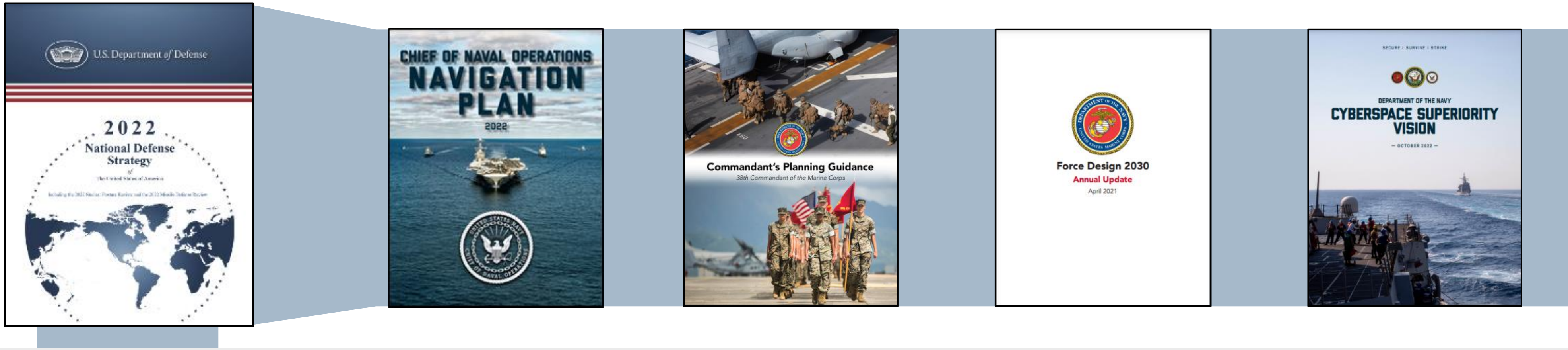
- Organizationally structured to pursue the best minds from across the nation and around the globe
  - Can fund academia, small businesses, industry, and government labs on topics of **naval relevance**
  - Broad BAA authorities to use the best performer for the job
  - Command manages 6.1, 6.2, 6.3 budget and SBIR, MURI, YIP, DURIP, and STEM programs for the Department of Navy (DoN)

> "ONR's mission is to plan, foster, and encourage scientific research in recognition of its paramount importance as related to the maintenance of future naval power, and the preservation of national security."
>
> PUBLIC LAW 588, APPROVED 1 AUG 1946

ONR Program Officer’s Role in Cyber S&T

OVERARCHING DRIVER:

Department of Navy (DoN) Strategic Guidance


U.S. Department of Defense
2022
National Defense Strategy
of the United States of America
CHIEF OF NAVAL OPERATIONS
NAVIGATION PLAN
2022
Commandant’s Planning Guidance
38th Commandant of the Marine Corps
Force Design 2030
Annual Update
April 2021
SECURE | SURVIVE | STRIKE
DEPARTMENT OF THE NAVY
CYBERSPACE SUPERIORITY VISION
OCTOBER 2022

SCIENTIFIC AND TECHNOLOGICAL BREAKTHROUGHS IN COMPUTING

TECHNOLOGY TRENDS, PRESSURES, AND LIMITATIONS

EVOLVING CYBER THREATS

Resource and Acquisition sponsor needs and priorities

Warfare Enterprise’s S&T Objectives and Fleet Capability Gaps

Interagency Coordination

DOD CYBER COI

ONR Program Officers serve as Navy’s S&T Technical Leadership

Cyber S&T Efforts

ONR POs are responsible for:

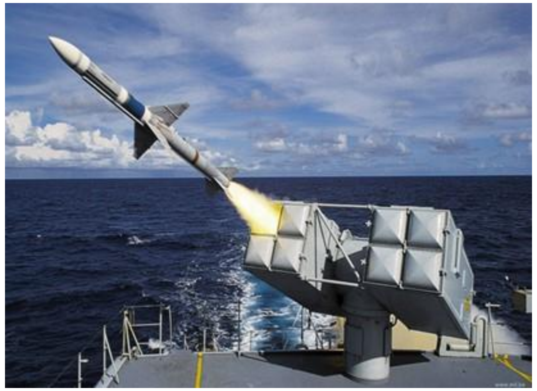
- Planning and executing naval cyber S&T investments to meet the needs of the future fleet
- Creating new programs, building support, transition

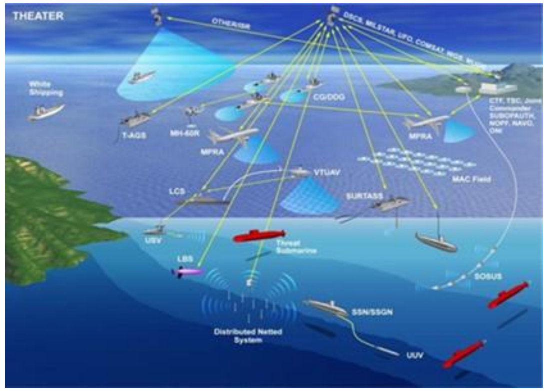
Now, about secure and resilient systems…

ONR's Emphasis: It's all about the mission!

Why (specifically) does the Navy need Secure and Resilient Systems?

- Computing systems that are capable of correctly executing the mission (within a user's tolerance of "correct") at/within the user's time of need.
  - A more nuanced / tailored approach to cybersecurity (than C-I-A, Scan & Patch, RMF, etc. etc.)
  - What is "Good Enough" for mission? May be highly context-dependent.
  - There is value in graceful degradation, reshaping cyber attack surface to buy time
  - Lots of S&T in: tailoring software *and tailoring security assessment* to mission





Our* prior talks at the summits

*and some of our performers'

- Physics-based framework for cyber resilience of CPS
  - See Nov 2020 talk by Ryan
- Software transformation and debloating
  - See Nov 2020 talk by Matt Mickelson
- Closer look at the drivers of software complexity and its impacts on trust
  - See Feb 2022 talk by Ryan
- Challenges/opportunities in modern software development
  - See May 2023 talk by Ryan
- Bottom-up Formal Methods
  - See talks from K. Hamlen Sept '19 & Nov '20 and Verbeek, Ravindran Sept '19

Also: Adam's DYKONDO poster at HCSS

Today I want to take a closer look at the incentive structure (& tools) that drives security decision making

Preliminaries

- Challenge: Incentivizing good security in the DoD acquisition base
  - E.g., “How do we get them to use our great tools?” “Why don’t they make better decisions?”
- A longstanding, difficult problem
- Ian Crone talked about it well in his keynote at the 2022 TCCoE Summit
  - Was speaking as the OUSD(R&E) Principal Director for Cyber
  - https://youtu.be/kvSgFaIC5zI
  - Constructing a broader ecosystem with the right incentives
  - “Victory looks like widespread use of these tools in the contractor base”

Imagine how many lines of code, 3rd party libraries, OS installs, vendor build chains, interconnects, etc. this translates to: →

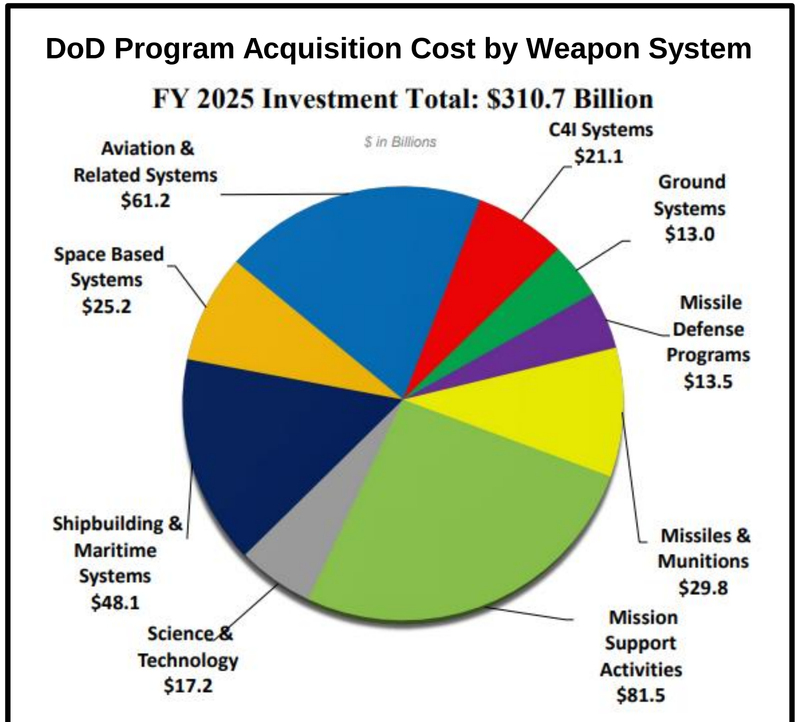
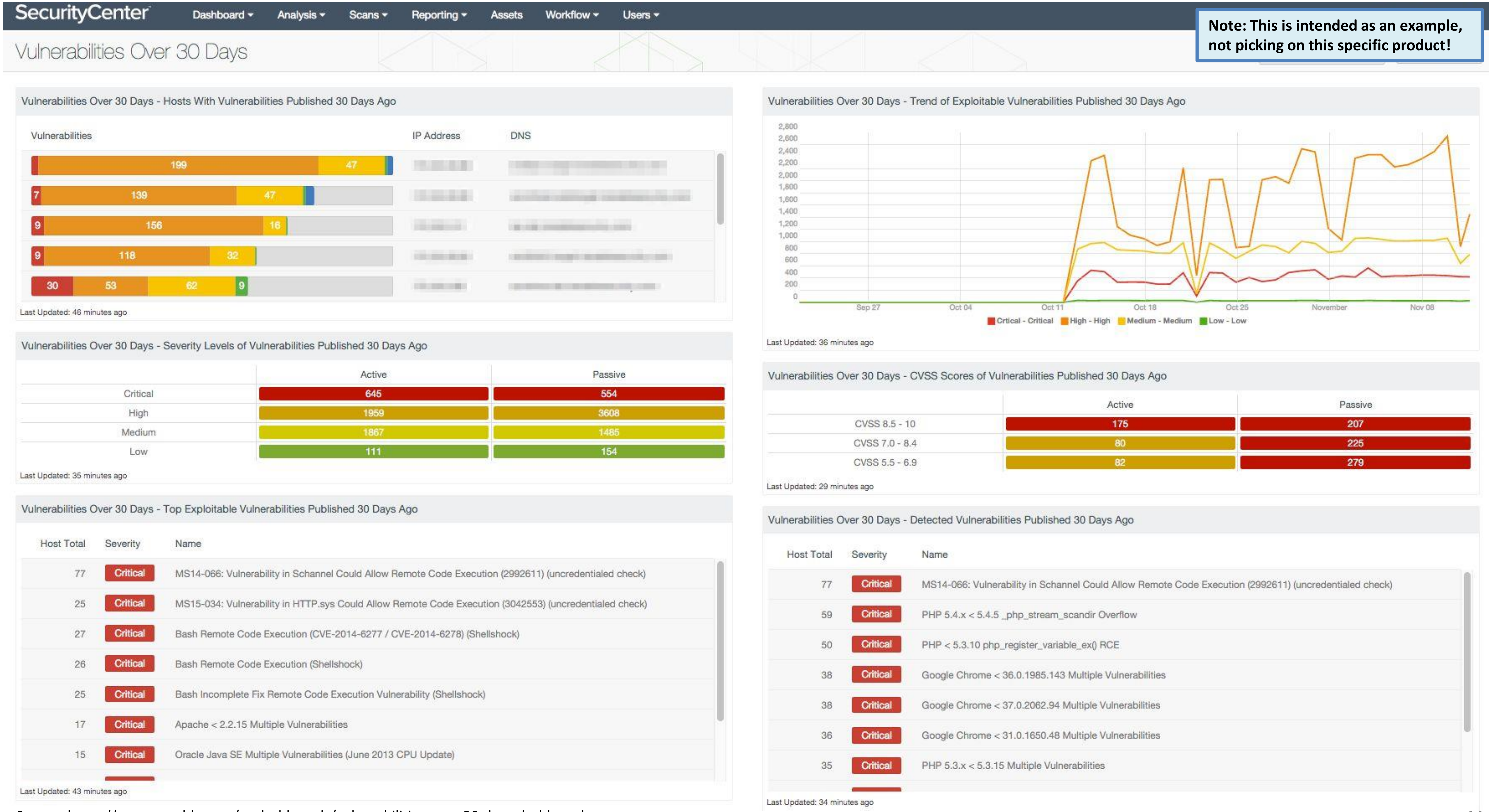


Figure from OUSD(Comptroller)

- My take: What is the biggest driver of security decisions (on the tool side)?



Note: This is intended as an example, not picking on this specific product!

Vulnerabilities Over 30 Days

Vulnerabilities Over 30 Days - Hosts With Vulnerabilities Published 30 Days Ago

Vulnerabilities	IP Address	DNS
199 · 47	[redacted]	[redacted]
7 · 139 · 47	[redacted]	[redacted]
9 · 156 · 16	[redacted]	[redacted]
9 · 118 · 32	[redacted]	[redacted]
30 · 53 · 62 · 9	[redacted]	[redacted]

Last Updated: 46 minutes ago

Vulnerabilities Over 30 Days - Trend of Exploitable Vulnerabilities Published 30 Days Ago

Last Updated: 36 minutes ago

Vulnerabilities Over 30 Days - Severity Levels of Vulnerabilities Published 30 Days Ago

	Active	Passive
Critical	645	554
High	1959	3608
Medium	1867	1485
Low	111	154

Last Updated: 35 minutes ago

Vulnerabilities Over 30 Days - CVSS Scores of Vulnerabilities Published 30 Days Ago

	Active	Passive
CVSS 8.5 - 10	175	207
CVSS 7.0 - 8.4	80	225
CVSS 5.5 - 6.9	82	279

Last Updated: 29 minutes ago

Vulnerabilities Over 30 Days - Top Exploitable Vulnerabilities Published 30 Days Ago

Host Total	Severity	Name
77	Critical	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)
25	Critical	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check)
27	Critical	Bash Remote Code Execution (CVE-2014-6277 / CVE-2014-6278) (Shellshock)
26	Critical	Bash Remote Code Execution (Shellshock)
25	Critical	Bash Incomplete Fix Remote Code Execution Vulnerability (Shellshock)
17	Critical	Apache < 2.2.15 Multiple Vulnerabilities
15	Critical	Oracle Java SE Multiple Vulnerabilities (June 2013 CPU Update)

Last Updated: 43 minutes ago

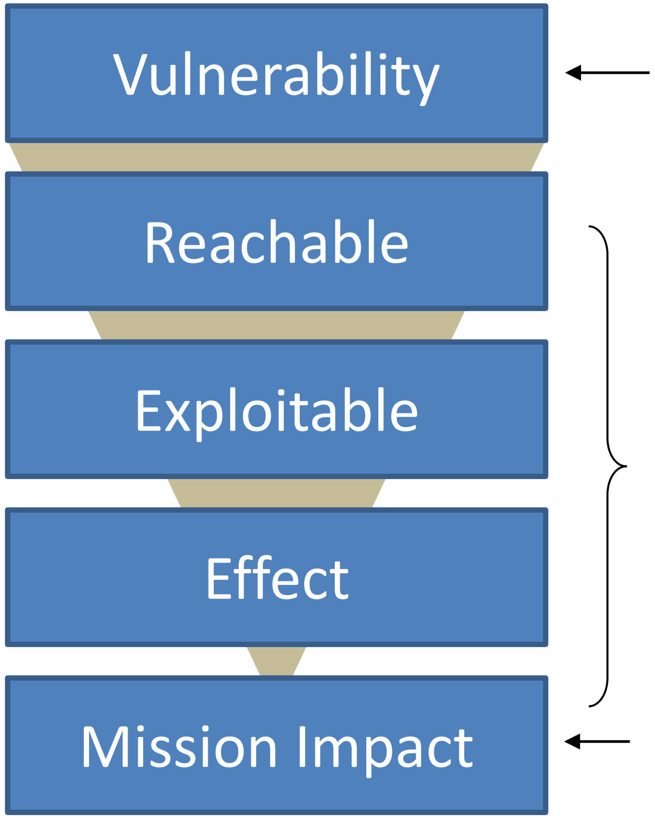
Vulnerabilities Over 30 Days - Detected Vulnerabilities Published 30 Days Ago

Host Total	Severity	Name
77	Critical	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)
59	Critical	PHP 5.4.x < 5.4.5 _php_stream_scandir Overflow
50	Critical	PHP < 5.3.10 php_register_variable_ex() RCE
38	Critical	Google Chrome < 36.0.1985.143 Multiple Vulnerabilities
38	Critical	Google Chrome < 37.0.2062.94 Multiple Vulnerabilities
36	Critical	Google Chrome < 31.0.1650.48 Multiple Vulnerabilities
35	Critical	PHP 5.3.x < 5.3.15 Multiple Vulnerabilities

Last Updated: 34 minutes ago

Source: https://www.tenable.com/sc-dashboards/vulnerabilities-over-30-days-dashboard

The Cyber Assessment Semantic Gap



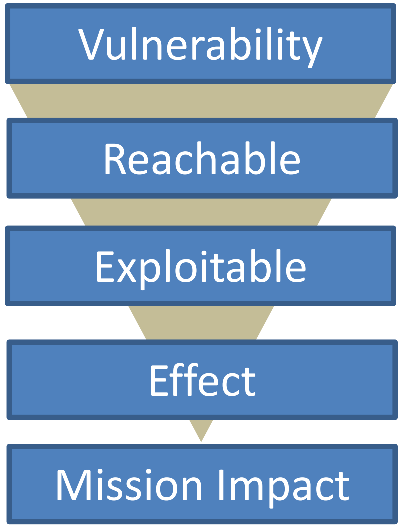
All the tools most accessible to acquisition teams measure here

- Also are the most commercially successful kinds of cyber assessment tools
- Further reinforced by their primacy in how we implement RMF / ATO

When assessed at
all, it is ad-hoc
and speculative

Meanwhile, this is what we really care about!

Major Limitations



Some Proactive Mitigations:

Software Debloating
Code order randomization
API Reshaping
Cyber Separable failover
SECCOMP filter employment
Compartmentalization
Micropatching
Tagged pointer integrity
Proactive vulnerability discovery
Secure-by-Design Techniques
Cyber-Resilient Digital Engineering
Supply chain inspection

- Focused on known / reported vulnerabilities (CVE-xxx)
- Severity levels often over/under estimate true risk of the bug
  - Ratings have big effect on people's behavior, but are often crudely defined
  - Time + resource-strapped PMs: "just get the CAT 1s and CAT 2s"
  - "Exploitability" Severity is often inferred / gleaned from the initial bug report
  - How the error is presented in the report depends on how the bug was triggered
  - For more, see: Lin, Zhenpeng, et al. "GREBE: Unveiling exploitation potential for Linux kernel bugs." 2022 IEEE Symposium on Security and Privacy (SP). IEEE, 2022.

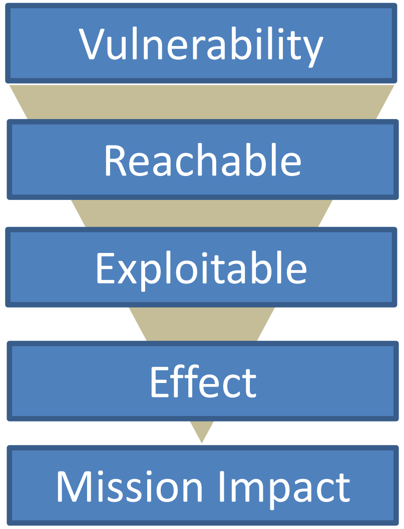
Out of 44 bot-reported kernel bugs they looked at:

- 26 had higher exploit potential than originally assessed
- 6 were turned into fully exploitable kernel vulnerabilities
- CVE-2021-3715 (UAF) Base Score: 7.8 HIGH — was originally rated low

- Fails to measure "exploit impedance" effects of proactive mitigations
- Not holistic. Focused on individual systems, individual containers, etc.

Underlying Implicit Assumptions

- So why do we do it this way?
  - Commercial viability
  - Better than nothing / "a good start"
  - Now, it is so tightly woven into standard risk management processes
- How could it be conceived as sensible / rational:



Rationale behind current approach was founded on these implicit key assumptions:

1. Finding new vulnerabilities is difficult and time-consuming
2. Expertise to make them into stable exploits is exceedingly rare
3. We can largely get those experts to responsibly disclose
4. Testing an exploit against a specific target will be noisy (or at least observable in some way)
5. "Exploitation impedance" is 0, once an adversary has a working RCE we're toast

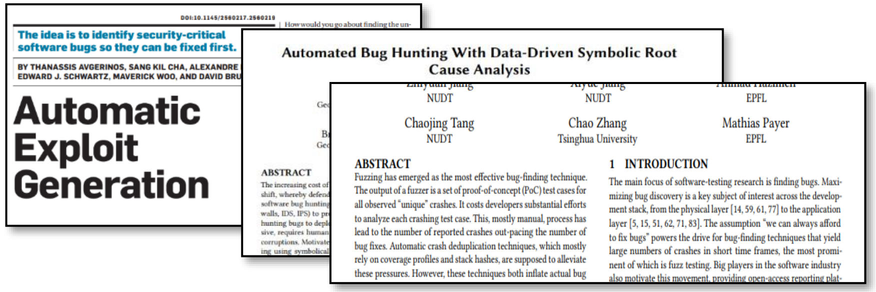
Flawed Assumptions => Invalid Rationale

☒ Finding new vulnerabilities is difficult and time-consuming

- Ex: Zerodium is paying only $1M for a Windows Zero Click RCE!

☒ Expertise to make them into stable exploits is exceedingly rare

- Automated techniques have advanced drastically
- Code keeps getting bigger and more complex



DOI:10.1145/2560217.2560219

The idea is to identify security-critical software bugs so they can be fixed first.

BY THANASSIS AVGERINOS, SANG KIL CHA, ALEXANDRE
EDWARD J. SCHWARTZ, MAVERICK WOO, AND DAVID BRU

How would you go about finding the un-

Automatic Exploit Generation

Automated Bug Hunting With Data-Driven Symbolic Root Cause Analysis

ABSTRACT
The increasing cost of
shift, whereby defend
software bug hunting
walls, IDS, IPS) to pr
hunting bugs to depl
sive, requires human
corruptions. Motivate
ing using symbolical

NUDT | NUDT | EPFL

Chaojing Tang, NUDT | Chao Zhang, Tsinghua University | Mathias Payer, EPFL

ABSTRACT

Fuzzing has emerged as the most effective bug-finding technique. The output of a fuzzer is a set of proof-of-concept (PoC) test cases for all observed "unique" crashes. It costs developers substantial efforts to analyze each crashing test case. This, mostly manual, process has lead to the number of reported crashes out-pacing the number of bug fixes. Automatic crash deduplication techniques, which mostly rely on coverage profiles and stack hashes, are supposed to alleviate these pressures. However, these techniques both inflate actual bug

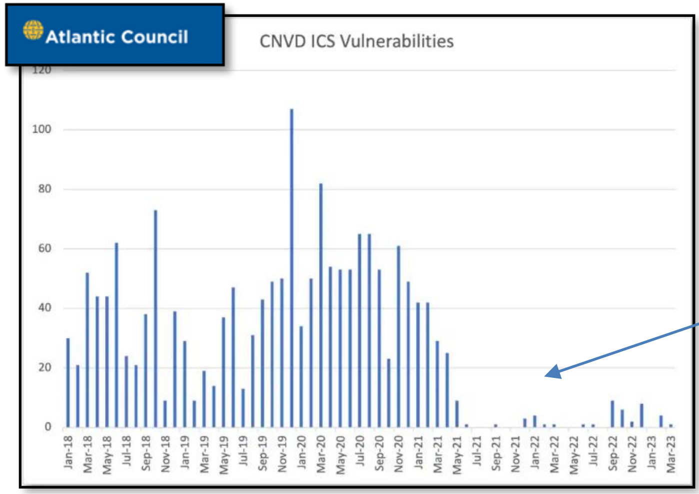
1 INTRODUCTION

The main focus of software-testing research is finding bugs. Maximizing bug discovery is a key subject of interest across the development stack, from the physical layer [14, 59, 61, 77] to the application layer [5, 15, 51, 62, 71, 83]. The assumption "we can always afford to fix bugs" powers the drive for bug-finding techniques that yield large numbers of crashes in short time frames, the most prominent of which is fuzz testing. Big players in the software industry also motivate this movement, providing open-access reporting plat-

☒ We can largely get those experts to responsibly disclose

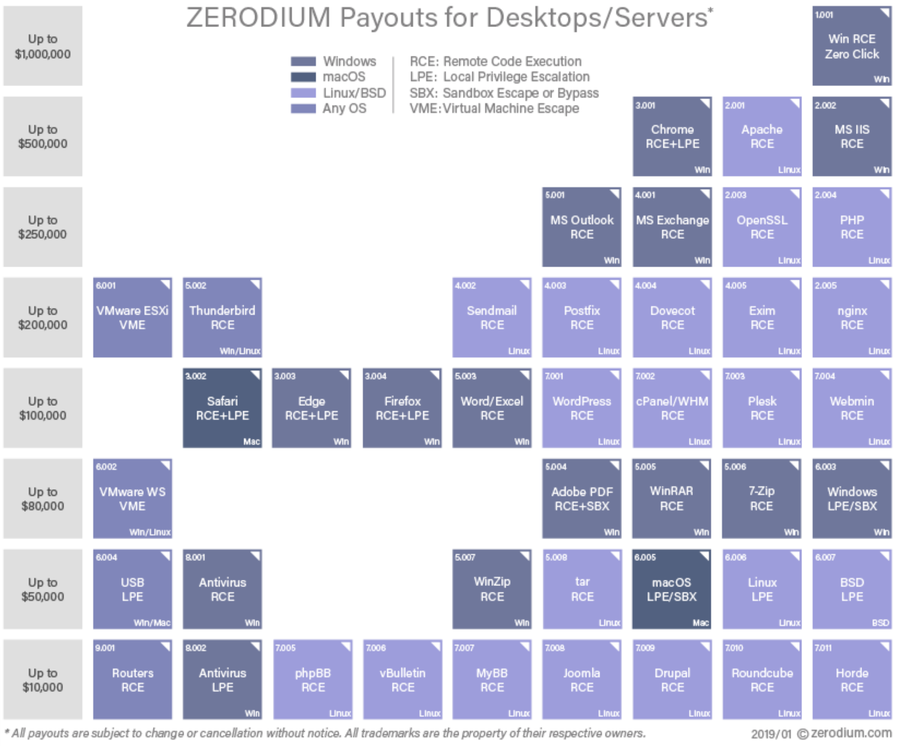
- See report published Sept 2023 by The Atlantic Council, *Sleight of Hand*
- In 2017 attitudes began shifting:
  e.g, Vulns are "important strategic resources"
- July 2021: New law (RMSV) requiring citizens to disclose bugs to government
- 2022 Microsoft report showed uptick in the number of 0-days used by nation-state hacking groups

https://www.atlanticcouncil.org/in-depth-research-reports/report/sleight-of-hand-how-china-weaponizes-software-vulnerability/



"…publication of vulnerabilities for industrial control systems ground to a halt in 2022"

Weaponized zero-days are plentiful…



ZERODIUM Payouts for Desktops/Servers*

Windows | macOS | Linux/BSD | Any OS

RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
VME: Virtual Machine Escape

Up to $1,000,000									1.001 Win RCE Zero Click Win
Up to $500,000							3.001 Chrome RCE+LPE Win	2.001 Apache RCE Linux	2.002 MS IIS RCE Win
Up to $250,000						5.001 MS Outlook RCE Win	4.001 MS Exchange RCE Win	2.003 OpenSSL RCE Linux	2.004 PHP RCE Linux
Up to $200,000	6.001 VMware ESXi VME	5.002 Thunderbird RCE Win/Linux			4.002 Sendmail RCE Linux	4.003 Postfix RCE Linux	4.004 Dovecot RCE Linux	4.005 Exim RCE Linux	2.005 nginx RCE Linux
Up to $100,000		3.002 Safari RCE+LPE Mac	3.003 Edge RCE+LPE Win	3.004 Firefox RCE+LPE Win	5.003 Word/Excel RCE Win	7.001 WordPress RCE Linux	7.002 cPanel/WHM RCE Linux	7.003 Plesk RCE Linux	7.004 Webmin RCE Linux
Up to $80,000	6.002 VMware WS VME Win/Linux					5.004 Adobe PDF RCE+SBX Win	5.005 WinRAR RCE Win	5.006 7-Zip RCE Win	6.003 Windows LPE/SBX Win
Up to $50,000	6.004 USB LPE Win/Mac	8.001 Antivirus RCE Win			5.007 WinZip RCE Win	5.008 tar RCE Linux	6.005 macOS LPE/SBX Mac	6.006 Linux LPE Linux	6.007 BSD LPE BSD
Up to $10,000	9.001 Routers RCE	8.002 Antivirus LPE Win	7.005 phpBB RCE Linux	7.006 vBulletin RCE Linux	7.007 MyBB RCE Linux	7.008 Joomla RCE Linux	7.009 Drupal RCE Linux	7.010 Roundcube RCE Linux	7.011 Horde RCE Linux

* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

2019/01 © zerodium.com

https://zerodium.com/program.html

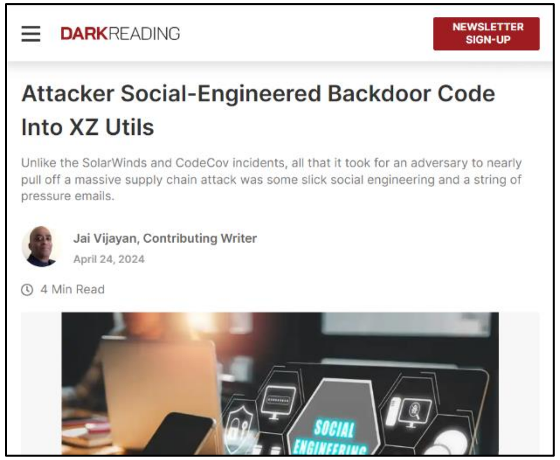
Flawed Assumptions => Invalid Rationale

☒ Testing an exploit against a specific target will be noisy/observable

- Most systems/apps extensively leverage 3rd party components that can be obtained elsewhere for cyber analysis
- Software supply chain offers pre-planning, pre-positioning opportunities, and have become more destructive and insidious the last few years

> "Actors leverage access to CDC networks to obtain sensitive data about U.S. defense and intelligence programs and capabilities."

From CISA Cybersecurity Advisory AA22-047A


DARKREADING

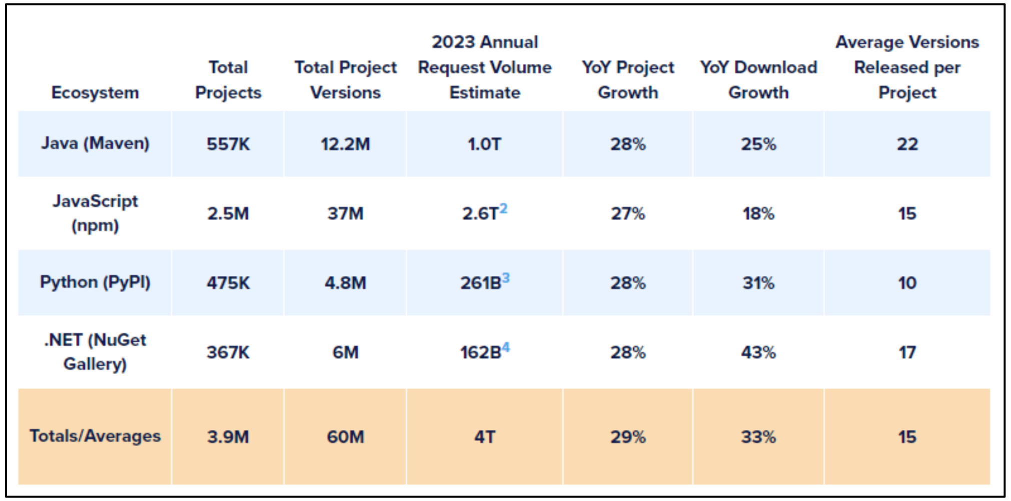
NEWSLETTER SIGN-UP

Attacker Social-Engineered Backdoor Code Into XZ Utils

Unlike the SolarWinds and CodeCov incidents, all that it took for an adversary to nearly pull off a massive supply chain attack was some slick social engineering and a string of pressure emails.

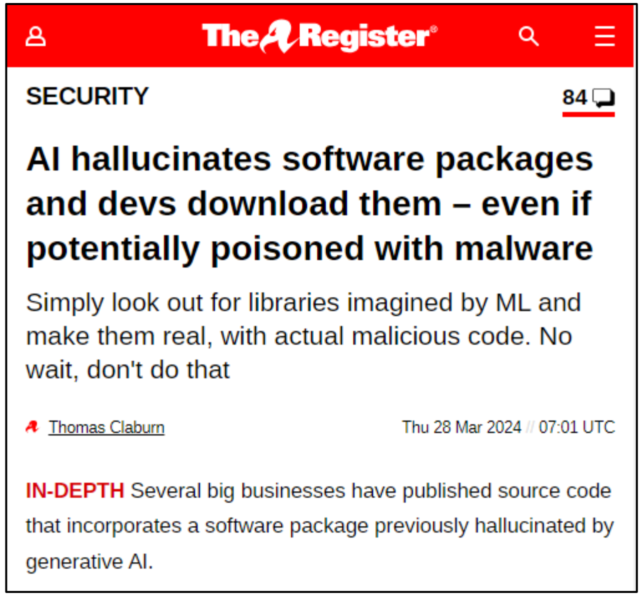
Jai Vijayan, Contributing Writer
April 24, 2024

4 Min Read



Ecosystem	Total Projects	Total Project Versions	2023 Annual Request Volume Estimate	YoY Project Growth	YoY Download Growth	Average Versions Released per Project
Java (Maven)	557K	12.2M	1.0T	28%	25%	22
JavaScript (npm)	2.5M	37M	2.6T[2]	27%	18%	15
Python (PyPI)	475K	4.8M	261B[3]	28%	31%	10
.NET (NuGet Gallery)	367K	6M	162B[4]	28%	43%	17
Totals/Averages	3.9M	60M	4T	29%	33%	15

Source: Sonatype, Software Supply Chain Stats 2023


The Register®

SECURITY 84

AI hallucinates software packages and devs download them – even if potentially poisoned with malware

Simply look out for libraries imagined by ML and make them real, with actual malicious code. No wait, don't do that

Thomas Claburn Thu 28 Mar 2024 // 07:01 UTC

IN-DEPTH Several big businesses have published source code that incorporates a software package previously hallucinated by generative AI.

☒ "Exploitation impedance" is 0

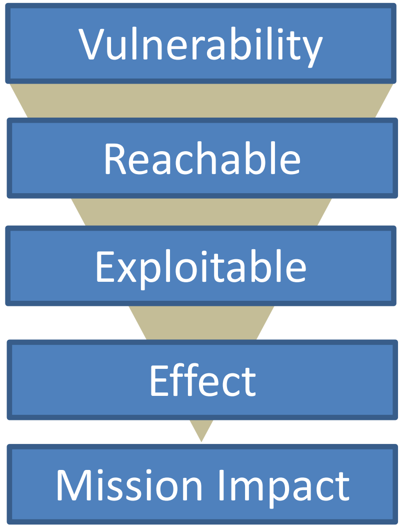
- S&T community has made tons of progress throughout the last decade developing proactive mitigation techniques that make it more difficult to convert vulnerability to pwn to mission effects. **(If they're put into use!)**

Software Debloating
Code order randomization
API Reshaping
Cyber Separable failover
SECCOMP filter employment
Compartmentalization

Micropatching
Tagged pointer integrity
Proactive vulnerability discovery
Secure-by-Design Techniques
Cyber-Resilient Digital Engineering
Supply chain inspection

Slide is UNCLASSIFIED – Distribution Statement A

So where does this leave us?



Vulnerability

Reachable

Exploitable

Effect

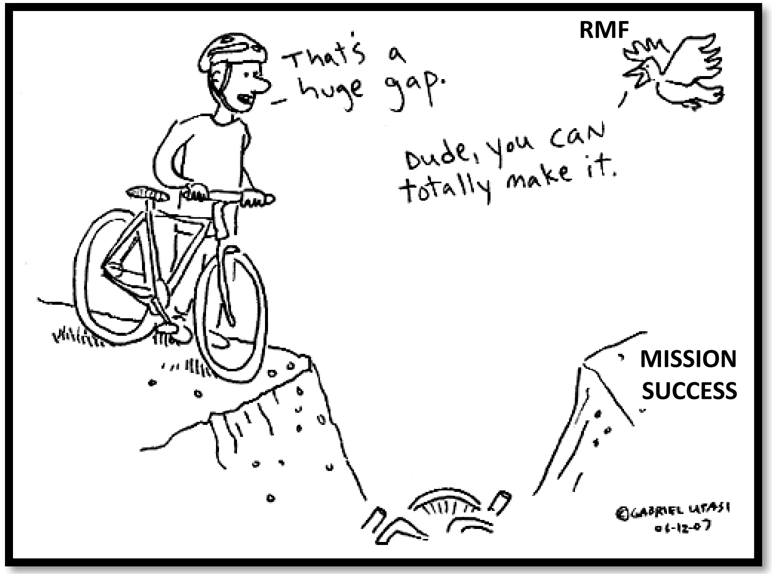
Mission Impact

Rationale behind current approach was founded on these implicit key assumptions:

1. ~~Finding new vulnerabilities is difficult and time-consuming~~
2. ~~Expertise to make them into stable exploits is exceedingly rare~~
3. ~~We can largely get those experts to responsibly disclose~~
4. ~~Testing an exploit against a specific target will be noisy (or at least observable in some way)~~
5. ~~"Exploitation impedance" is 0, once an adversary has a working RCE we're toast~~

Every single one of these is no longer true!
(to the extent that it ever was)

The gap between our existing process of managing known vulnerabilities and understanding mission risk posed by non-kinetic warfighting has never been wider



Where would we like to go?

- Incumbent upon the S&T community to chart a better path that is:
  - Mission-centric and readiness-oriented
  - More dynamic (and response to how broader changes affect security posture)
  - More holistic (in recognition that complex systems are not just a single app)
  - More cooperative with the reality of the economics trade space
    - Cyber security investments often require PMs to trade risk on cost, schedule, and performance

ONR looking to support novel research into:

- New means of handling cyber information: multi-modal, machine curated and machine readable, informed by and substantiated by dynamic iterations of static/dynamic program and network analysis
- System(s)-of-systems characterization tools, high-fidelity across components and across modalities
- New ways to derive operational intent (mission) from limited available external information
- Analysis and understanding tools to define cascading effects of cyber actions, exploit chain metrics
- Visualization models that ground acquisition decision making with operational objectives

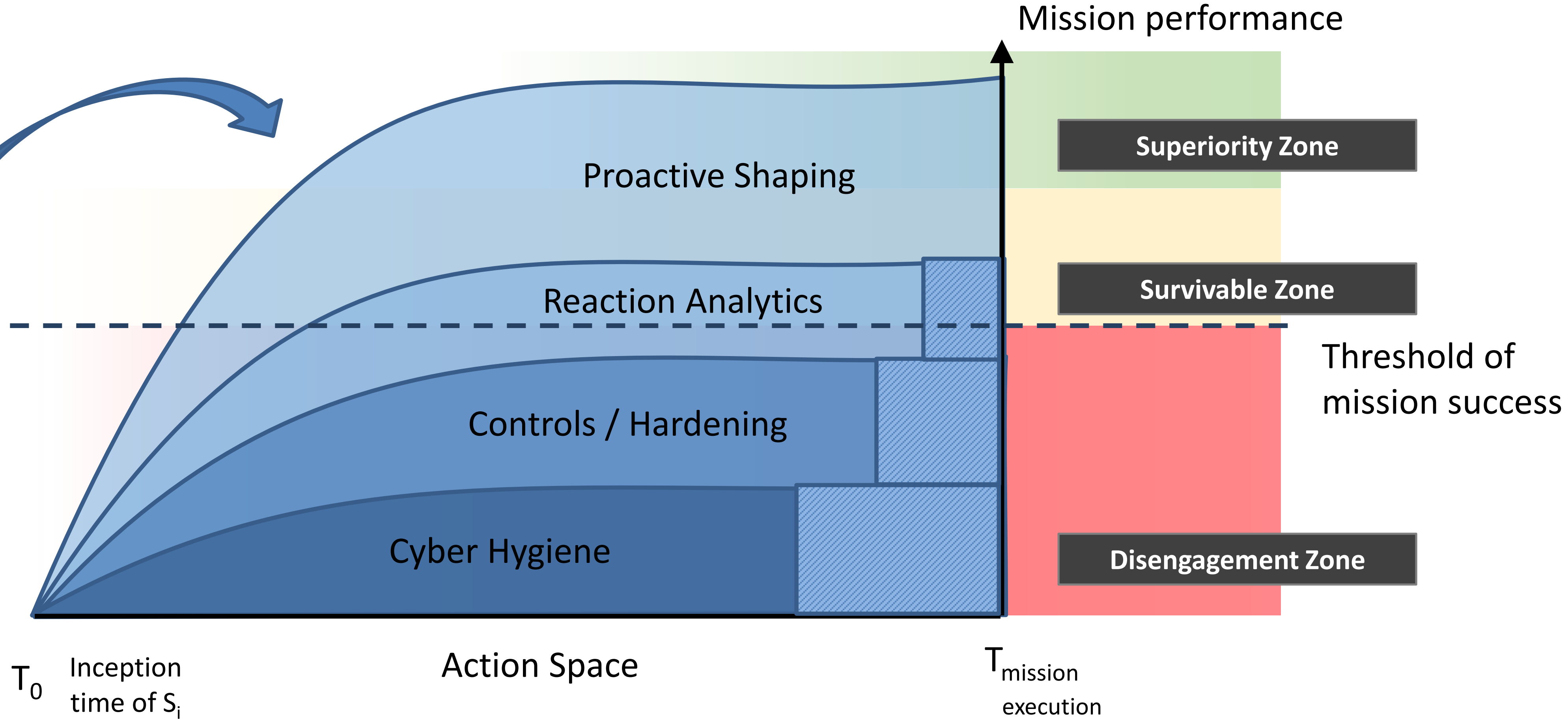
In addition to getting after the S&T, this venture ultimately needs a technical authority to lead (maybe this is something JFAC can do?)

- DIB outreach and awareness
- Tools clearinghouse (that S&T can transition to)
- Configuration control of the assessment methodologies
- Continuous trade studies and scientifically rigorous studies to back up / reshape recommendations and scoring measures
- Provide advice from experts
- Cyber policy to cement the office and its products as a must-do for DoD weapon system builders
- Policy must relax other burdens (challenge existing RMF / ATO structures)

Example visualization model:

Living Battlespace Performance (LBP) model

- Need model capable of handling **unquantifiable uncertainties**



Potential to be much bigger than other curves:

Software Debloating
Code order randomization
API Reshaping
Cyber Separable failover
SECCOMP filter employment
Compartmentalization
Micropatching
Tagged pointer integrity
Proactive vulnerability discovery
Secure-by-Design
Cyber-Resilient Digital Engr.
Zero-trust of the supply chain

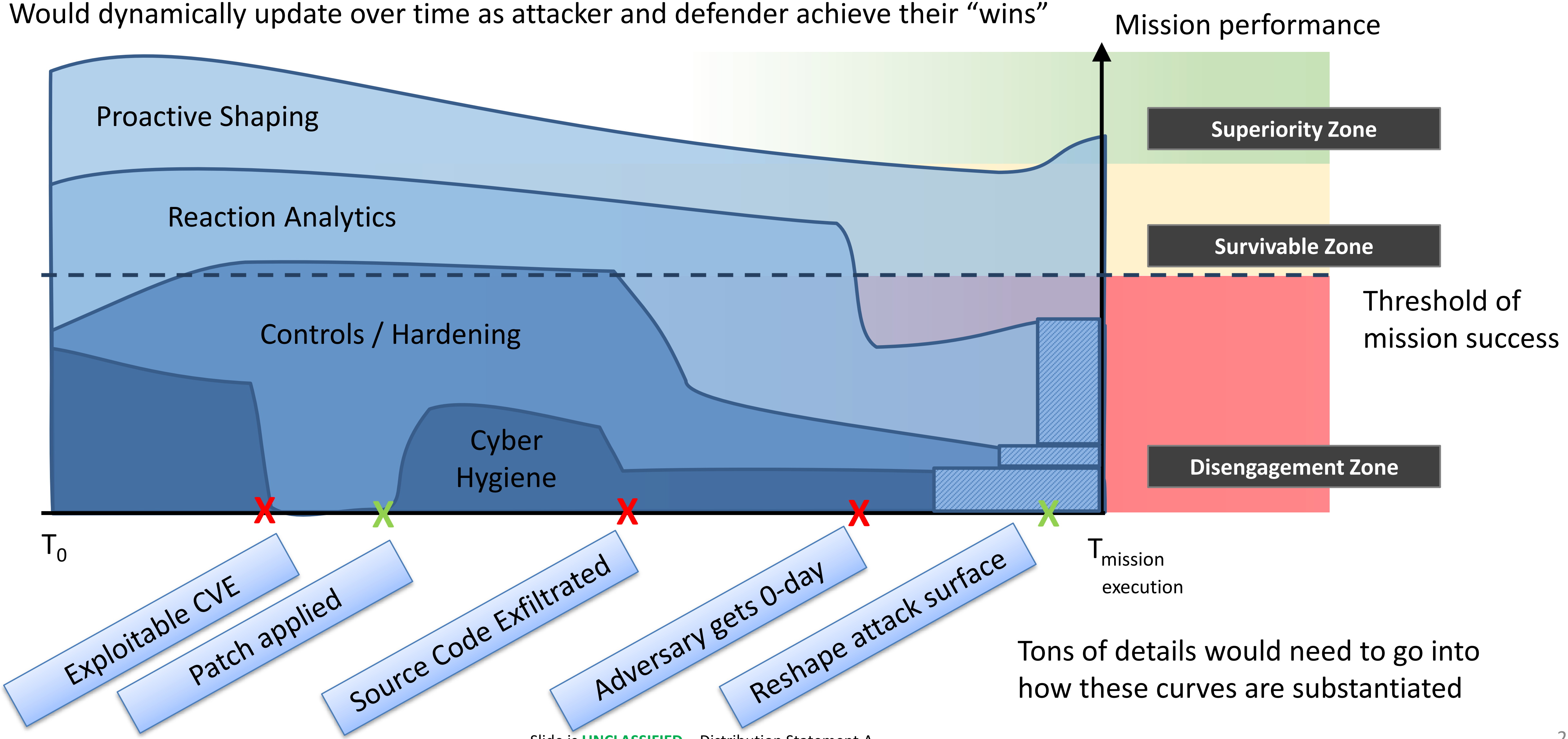
- Action space incorporates adversary “wins” and defender “wins” over system life
- Allows for strategizing into future, game out the effects of different investment strategies on mission performance in the face of adversarial cyber interference

– Implant added in software supply chain
– New ‘feature’ added that later becomes bug
– Exposure of source code
– Adversary gets new analysis capabilities

Example visualization model:

Living Battlespace Performance (LBP) model

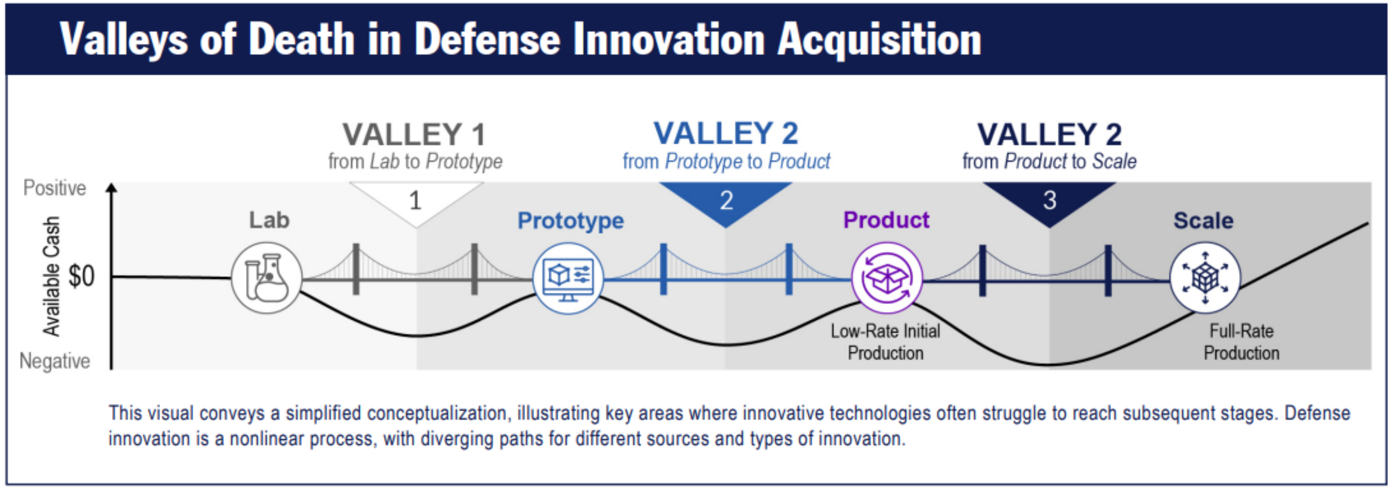
- Would dynamically update over time as attacker and defender achieve their “wins”



Tons of details would need to go into how these curves are substantiated

Takeaways

- Current Technology Advances and Modern Software Development
  - Still needs new means to incentivize adoption of latest security advances
  - New AI products see rapid adoption, excitement. Why? Offers a new feature.
  - For security: tie to new desirable feature sets, or alter the incentive structure
- We want to begin driving the community to a mission-focused cyber readiness approach
  - Beyond scan and patch
  - New assessment models
  - High-fidelity, ground-truth
  - Tailor attack surface measurement to the mission



Valleys of Death in Defense Innovation Acquisition

This visual conveys a simplified conceptualization, illustrating key areas where innovative technologies often struggle to reach subsequent stages. Defense innovation is a nonlinear process, with diverging paths for different sources and types of innovation.

2023 National Defense Science & Technology Strategy
https://www.cto.mil/wp-content/uploads/2023/05/2023-NDSTS.pdf

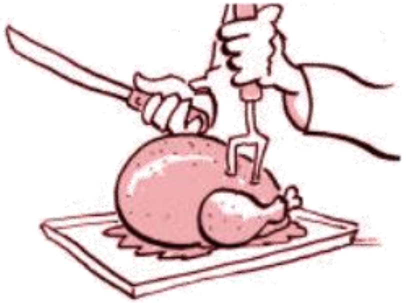
Applied Cyber Resiliency Program

Research Concentration Areas

- Safe and Resilient Cyber-Physical Systems
  - Tolerate and survive adversarial cyber interference
- Understanding and Limiting the Exploitability of Systems
  - Reduce and reshape attack surfaces
  - Protect system elements not traditionally considered by cybersecurity
- Advancing Automation of Cyber Operations
  - Defend in disadvantaged and intermittent environments
- Transformation and Analysis to achieve Zero-trust Hardware and Software Supply Chains
  - Limit the opaque and unchecked sources of brittleness in our systems

https://www.nre.navy.mil/organization/departments/code-31/division-311/applied-cyber-resiliency

Group inbox: **usn.pentagon.cnr-arlington-va.mbx.ONRCyber@us.navy.mil**



Advertisement: FEAST

- FEAST: Forming an Ecosystem Around Software Transformation
- 6th one in series. We started it in 2016. First one since 2020.
- To be held **Friday, October 18, 2024** in Salt Lake City, UT
  - Co-located with ACM CCS
- Check out our CFP, now posted online here:

https://feastworkshop.github.io

- Papers Due July 17!

Slide is UNCLASSIFIED – Distribution Statement A