

# Using AI to Enhance Cybersecurity

V.S. Subrahmanian  
Northwestern Security & AI Lab  
[vss@northwestern.edu](mailto:vss@northwestern.edu)

June 6 2023  
Indo-Pacific GeoIntelligence

# Talk Outline

1

Northwestern Cyber  
Early Warning  
System: NCEWS

2

Estimate Malware  
Spread

3

Deter IP Theft

4

Deepfakes

5

NATO Locked Shields  
Research

# Cyber Early Warning Systems

**New Vulnerability  
Discovered**

**Will it be used in a  
real-world exploit?**

**If yes, how far into the  
future?**

**How severe will it be?**

What percentage of discovered vulnerabilities are used in an attack?

What percentage of known vulnerabilities are used in an attack before NIST releases their assessment (CVSS) ?

**The faster these questions can be answered, the safer the enterprise will be**

# Cyber Early Warning Systems

New Vulnerability  
Discovered

Will it be used in a  
real-world exploit?

> 95 % F1-score

If yes, how far into the  
future?

+/- 11.9 days error

How severe will it be?

+/- 1.25 error on a  
10 point scale

What percentage of discovered vulnerabilities are used in an attack? **9.2%**

What percentage of known vulnerabilities are used in an attack before NIST releases their assessment (CVSS) ? **49.46%**

The faster these questions can be answered, the safer the enterprise will be

# NCEWS Screenshots

**Situations change, fast. Good thing we keep up.**  
Predictive analytics get security professionals ahead. Check out how we help with real-time decision-making.

**CVE-2022-28662**  
A vulnerability in the user interface of Microsoft Exchange (CVE-2022-28662) allows an attacker to bypass authentication and gain access to the mailbox folder as a local administrator without requiring user interaction.

**CVE-2022-28778**  
Integer overflow vulnerability in Microsoft Security Scanner prior to version 1.0.432 allows an attacker to gain the ability to execute code as a local administrator without requiring user interaction.

**CVE-2022-1282**  
A command injection vulnerability in the process when an attacker with access to the console command can execute arbitrary commands on the system.

**U.S. Says It Secretly Removed Malware Worldwide, Preempting Russian Cyberattacks**  
WASHINGTON — The United States said on Wednesday that it had secretly removed malware from computer networks around the world to ward off attacks, which the president said were Russian cyberattacks and sent a message to President.

**CrowdStrike**  
CrowdStrike says it has removed malware from its servers in the United States and other countries. The company says it has removed malware from its servers in the United States and other countries.

**CVE-2020-32987**

**Predictions**

**9.4** This severity score prediction indicates that this CVE poses an extremely large system vulnerability risk. [View details >](#)

**60 days** This days to exploit prediction indicates that this CVE should be a high priority to address since it is likely that it will be exploited within the next 3 months. [View details >](#)

**80%** This likelihood prediction indicates that this CVE has a very high likelihood of being exploited. [View details >](#)

**Distributions**

**Table View**

CVE	Patch priority	CVSS prediction	Days to exploit	Severity of exploit
2020-32987	Very high	9.7	14 days	Very high
2020-33287	Very high	9.1	7 days	High
2020-32987	High	8.7	30 days	High
2020-39987	High	8.5	64 days	Very high
2020-39112	High	8.5	57 days	High
2020-39168	High	8.4	7 days	Moderate
2020-23210	High	8.2	12 days	Moderate
2020-45112	High	8.2	12 days	Very high
2020-45112	Moderate	7.8	40 days	Moderate

**Dashboard**

**Chart View**

**Table View**

CVE	Patch priority	CVSS prediction	Days to exploit	Severity of exploit
2020-32987	Very high	9.7	14 days	Very high
2020-33287	Very high	9.1	7 days	High
2020-32987	High	8.7	30 days	High
2020-39987	High	8.5	64 days	Very high
2020-39112	High	8.5	57 days	High
2020-39168	High	8.4	7 days	Moderate
2020-23210	High	8.2	12 days	Moderate
2020-45112	High	8.2	12 days	Very high
2020-45112	Moderate	7.8	40 days	Moderate



# Estimating Malware Spread

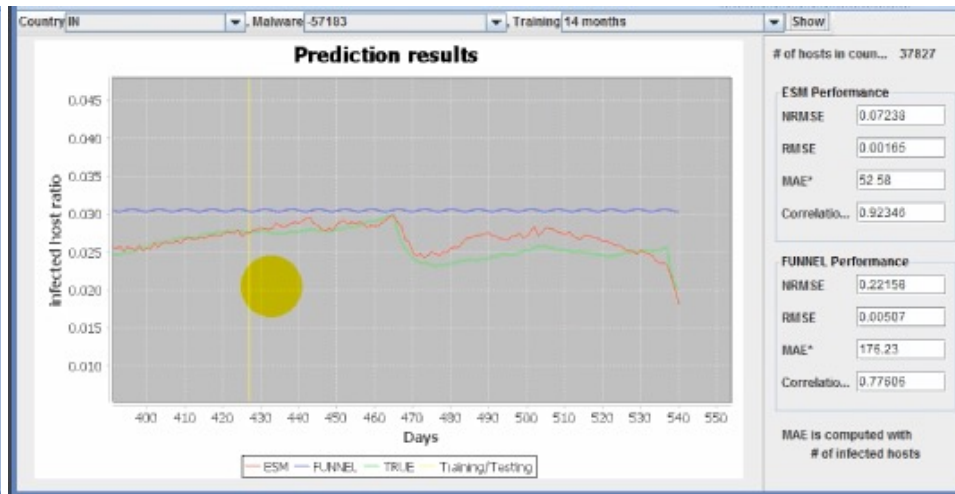
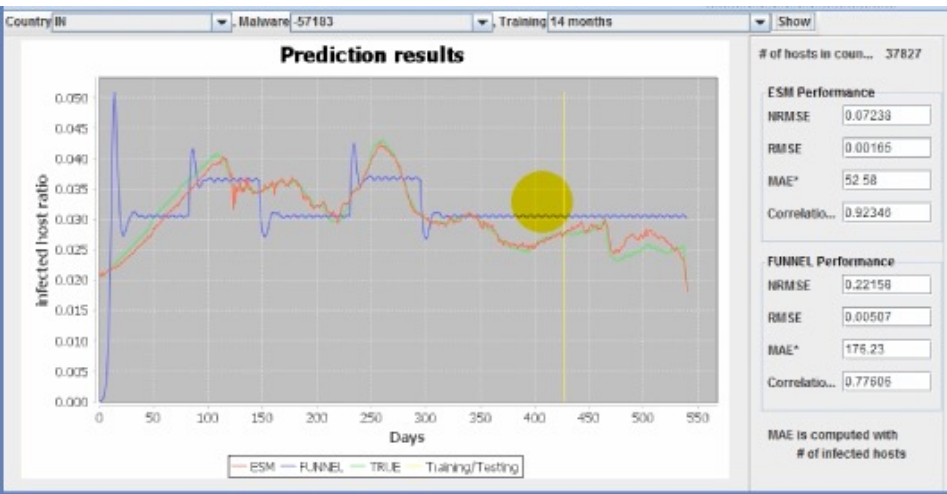
**New Malware  
Discovered**

**What percentage  
of hosts in my  
network will be  
hit?**

**What percentage  
of high asset  
value hosts will be  
hit?**

**How best can we  
mitigate this  
spread?**

# Estimating Malware Spread



Using data from Symantec

# Deterring IP Theft with Fakes

## Sentences from Restaurant Reviews

1. decent black coffee and good service
2. authentic tasting sauce, fresh crust

## Sentences from Movie Reviews

3. Russell Crowe's direction is far too predictable
4. the movie just feels dry and generic and very narrow all around

## Scientific Paper Titles

5. sequential depth quantization method for large-scale reconstruction
6. parsing and ensemble of deep convolutional neural network models

**Which are real which are fake?**



# Generating Fakes to Deter IP Theft

## Sentences from Restaurant Reviews

1. decent black coffee and good service
2. authentic tasting sauce, fresh crust

## Sentences from Movie Reviews

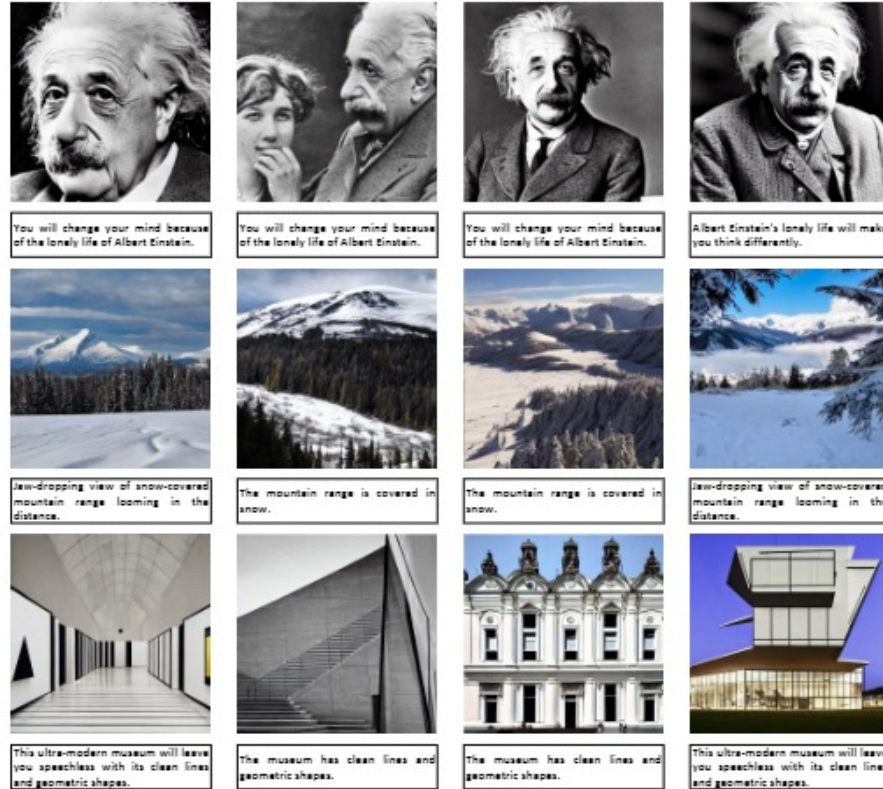
3. Russell Crowe's direction is far too predictable
4. the movie just feels dry and generic and very narrow all around

## Scientific Paper Titles

5. sequential depth quantization method for large-scale reconstruction
6. parsing and ensemble of deep convolutional neural network models

**Sentences in red are fake**

# Generating Multimodal Fakes



**Extended to handle data theft as well**

# Identifying Suspicious Sessions in the NATO Locked Shields Exercise

Huge cybersecurity exercise (32 countries, 2000+ participants in 2022)

1000+ servers on the Locked Shields network

Over 14M sessions of data. ~350K are malicious.

Goal: Find suspicious sessions. Fast.

Joint work with Netherlands Defence & TU Delft

# Some Prediction Results

Approach	AUC	Precision	Recall	F1-Score
SUS	<b>1</b>	1	1	<b>1</b>
Swiss <sup>1</sup>	0.999	0.604	1	0.753
Jan-Klein <sup>2</sup>	0.859	0.404	0.719	0.517

Approach	AUC	Precision	Recall	F1-Score
SUS	<b>0.99</b>	0.9	0.98	<b>0.938</b>
Swiss <sup>1</sup>	0.838	0.59	0.676	0.633
Jan-Klein <sup>2</sup>	0.75	0.386	0.505	0.438

Approach	AUC	Precision	Recall	F1-Score
SUS	<b>0.995</b>	0.699	0.99	<b>0.819</b>
Swiss <sup>1</sup>	0.874	0.437	0.75	0.55
Jan-Klein <sup>2</sup>	0.904	0.705	0.809	0.754

After 4 hours

After 8 hours

After 16 hours



- Predictions after
  - 4 hours
  - 8 hours
  - 16 hours
  - 32 hours
- Our **suspicion score** approach outperforms existing approaches in all settings

# Conclusion

- AI is already playing a major role in cyber-defense
  - Malware analysis and detection
  - Corporate risk posture
  - Intellectual property protection, data breaches
- The role of AI is poised to grow in coming years.
  - Generating and detecting phishing messages and posts
  - Generating and detecting infected URLs
  - Generating and detecting attack graphs
  - Generating and detecting malware

# Contact Information

V.S. Subrahmanian  
Walter P. Murphy Professor of Computer Science  
Buffett Faculty Fellow – Buffett Institute of Global Affairs  
Northwestern University  
1800 Sherman Ave, Suite 3-000  
Evanston, IL 60201.

[vss@northwestern.edu](mailto:vss@northwestern.edu)

<https://vssubrah.github.io/>

The screenshot shows the Amazon product page for the book "The Android Malware Handbook: Manual Analysis and ML-Based Detection Kindle Edition". The page includes the Amazon logo, navigation menu, and product details. The book is priced at \$29.99 for the Kindle edition and \$49.99 for the paperback. The author is V.S. Subrahmanian, and the publisher is Penguin Random House. The page also features a "Pre-order" button and a "Follow the Author" link.

amazon.com/Android-Malware-Handbook-Analysis-Detection-ebook/dp/B0BZGZ5X5F/ref=sr\_1\_1?crd=3K9T9T5RB2UDZ&keywords=the+andr...  
the android malware handbook +porst  
Hello, sign in Account & Lists Returns & Orders Cart  
All Clinic Best Sellers Customer Service Amazon Basics New Releases Prime - Music Today's Deals Books Registry Fashion Amazon Home Pharmacy Gift Cards One Medical Hot summer deals  
Buy a Kindle Kindle eBooks Kindle Unlimited Prime Reading Best Sellers & More Categories Kindle Vella Amazon Book Clubs Kindle Book Deals Kindle Singles Newsstand Manage content and devices Advanced Search  
CPT 2022: Professional Edition 5.0 960 \$68.99 prime  
Back to results  
The Android Malware Handbook: Manual Analysis and ML-Based Detection Kindle Edition  
by Qian Han (Author), Sai Deep Tetali (Author), Salvador Mandujano (Author), Sebastian Porst (Author), V.S. Subrahmanian (Author)  
Format: Kindle Edition  
See all formats and editions  
Kindle \$29.99 Read with Our Free App  
Paperback \$49.99 1 New from \$49.99  
Written by machine-learning researchers and members of the Android Security team, this all-star guide tackles the analysis and detection of malware that targets the Android operating system.  
This comprehensive guide to Android malware introduces current threats facing the world's most widely used operating system. After exploring the history of attacks seen in the wild since the time Android first launched, including several malware families previously absent from the literature, you'll practice static and dynamic approaches to analyzing real malware specimens. Next, you'll  
Read more  
Follow the Author  
Pre-order Price: \$24.88 includes free international wireless delivery via Amazon Whispernet  
Sold by: Penguin Random House Publisher Services  
Price set by seller.  
Pre-order with 1-Click\*  
This title will be auto-delivered to your Kindle on November 7, 2023.  
eBook features:  
• Highlight, take notes, and search in the book  
Deliver to your Kindle Library  
Add to List