Trailblazing the Artificial Intelligence for Cybersecurity Discipline:
Overview of the Field and Future Trends

Sagar Samtani, Ph.D.

Assistant Professor, Grant Thornton Scholar, and CACR Fellow

Kelley School of Business, Indiana University

Outline

- My Background
- Objective and Disclaimers
- An Overview of AI for Cybersecurity
- Sample AI for Cybersecurity Research Illustration
- Workforce Development, Archival Mechanisms, and Funding Opportunities
- Conclusion

My Background

- Assistant Professor of Operations and Decision Technologies (ODT) in the Kelley School of Business at Indiana University.
  - Ph.D. (2018), MS (2014), BS (2013) in MIS from University of Arizona.
  - NSF Scholarship-for-Service (SFS) fellow from 2014 – 2017.

- Research and Education Interests:
  - **Domain** – cybersecurity cyber threat intelligence, AI for cybersecurity, scientific cyberinfrastructure cybersecurity
  - **Methods** – AI deep learning, network science, data/text/web mining, visualization

Objective(s)

- **The objective of this talk is three-fold:**
  - Introduce the role of AI for cybersecurity;
  - Provide a background of existing initiatives;
  - Summarize potential mechanisms to progress the discipline.

Disclaimers!

- **Disclaimer 1:** I do not know everything.
- **Disclaimer 2:** The views and opinions in these slides reflect mine only and may change or evolve.
- **Disclaimer 3:** When presented live, these slides are supplemented by numerous examples of the concepts described.
  - However, the slides are sufficiently detailed such that readers can extract the main points without a live presentation.

Outline

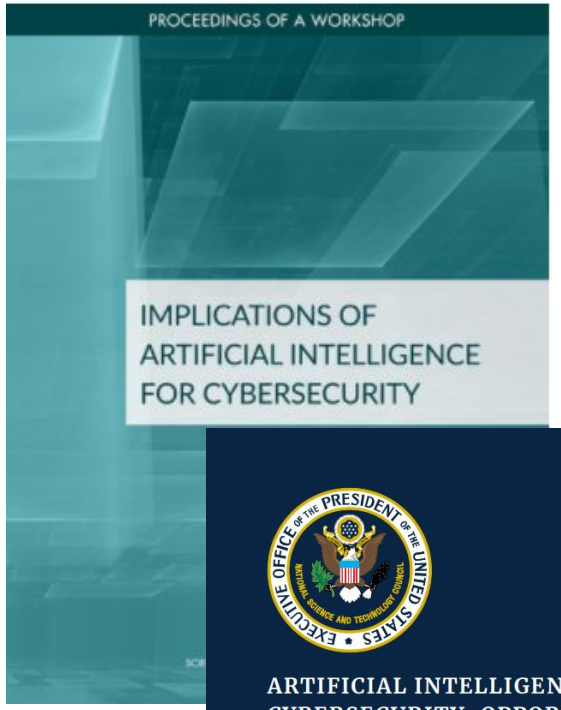
- My Background
- Objective and Disclaimers
- An Overview of AI for Cybersecurity
- Sample AI for Cybersecurity Research Illustration
- Workforce Development, Archival Mechanisms, and Funding Opportunities
- Conclusion

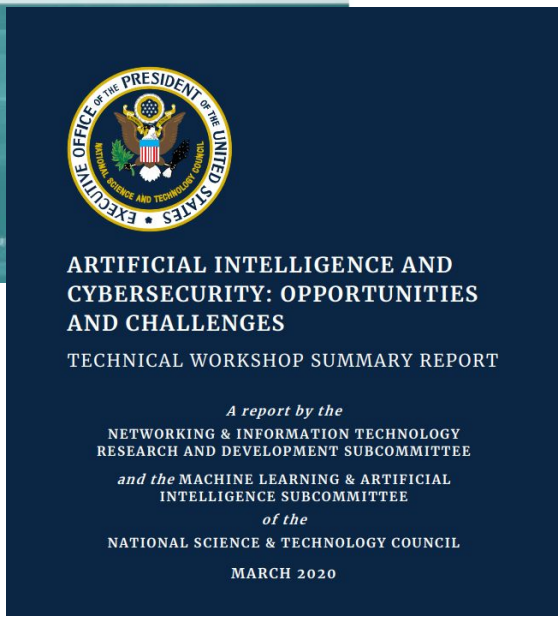
Cybersecurity and AI

- Common cybersecurity tasks asset identification, control allocation, vulnerability management, threat detection, etc.
  - Challenges data overload, limited human resources, etc.

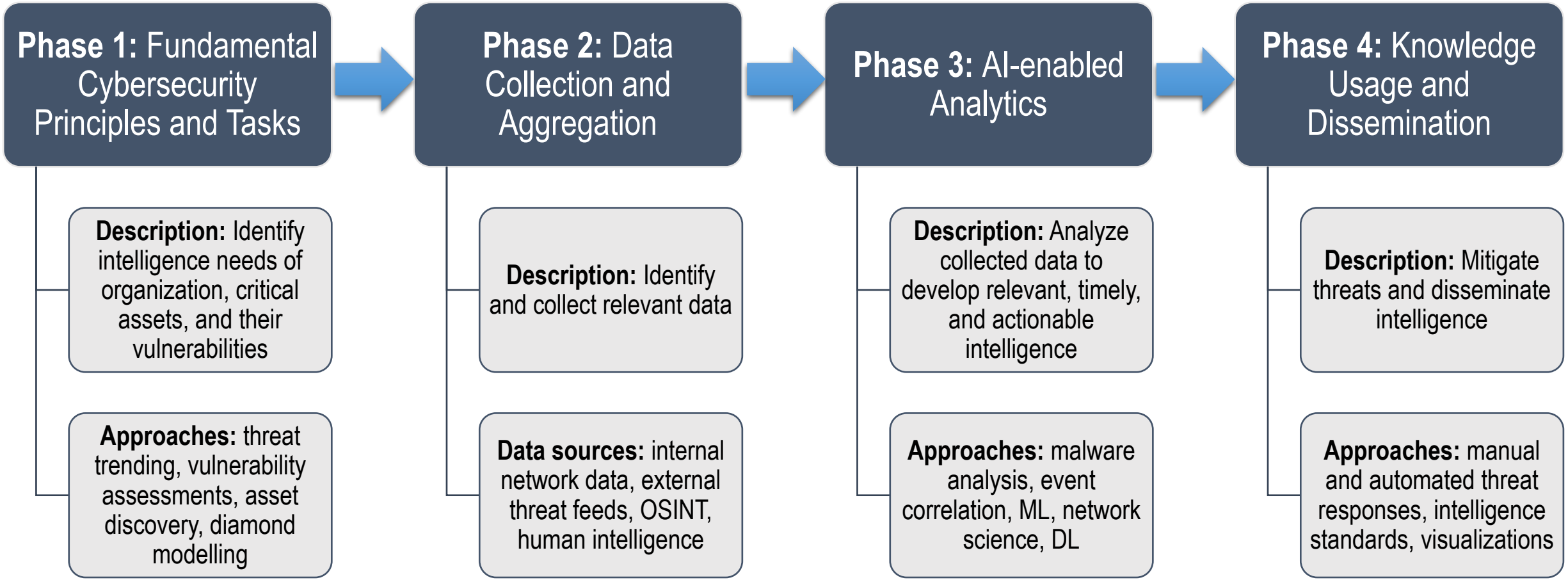
- AI and Cybersecurity not just buzzwords!
  - Noted as a national security priority by NSF, NSTC, and NAS.

- Role of AI for Cybersecurity is two-fold:
  1. Automate common cybersecurity tasks sift through data more efficiently and effectively than a human.
  2. Identify patterns in large datasets missed by manual analysis.





AI for Cybersecurity – A General Approach



Internal Cybersecurity Data Sources

Data Source	Example Platforms or Tools	Sample Metadata and Data
Workstations and/or VM images	Docker, containers, Vmware	Operating system, applications
Data storage	File store, disk drives, file directories	File size, directory name
Networking devices	Routers, switches, gateways, SDN software	ARP, routing tables
Network-based fingerprint data	Nmap, Zmap	TCP, packer header, UDP
Netflow data	-	Source, destination, bytes
Alert and event logs	Security information and event management	Date, alert name, IP address, action
Vulnerability assessments	BurpSuite, Nessus, Qualys, OpenVAS	Name, severity, risk
Biometric data	Mouse movements, eye movements, pulse	X-y-z axis accelerometer readings
Intranets	SharePoint, Confluence, Teams, Slack	Usernames, plain text

- **Characteristics of Internal (within an organization) Data:**
  - Close to the critical assets (e.g., servers, VMs, workstations) of many organizations.
  - Data is primarily machine generated high velocity, more standard formats.
  - Provides excellent insight about existing threats and past attacks.
  - Some of the most common data sources to be used for AI for cyber education.

External Cybersecurity Data Sources

Data Source	Example Platforms or Tools	Sample Metadata and Data
Social coding repositories	GitHub, SourceForge	Commits, authors, code, forks
IoT search engines	Shodan, Censys, Fofsa, BinaryEdge	IP, banner data, images, lat/long
Hacker forums	Antichat, Ciphers, WildersSecurity	Date, author, threads, source code
DarkNet marketplaces	Hansa, DreamMarket	Product name, author name, price
Internet-Relay-Chat	Anonops	Date, plain-text
Carding shops	JStash, Recator	Card type, zip code
Paste sites	PasteBin	Raw paste, author, date, size
Commercial threat feeds	AlienVault OTX	IPs, hashes, source, destination
Malware Repositories	EMBER, VirusTotal	Hash, binary, date, malware reports
News sources	CNN, BBC, Fox, ABC	Headlines, text bodies, images
Conventional social media	Twitter, Facebook, YouTube	Usernames, plain text

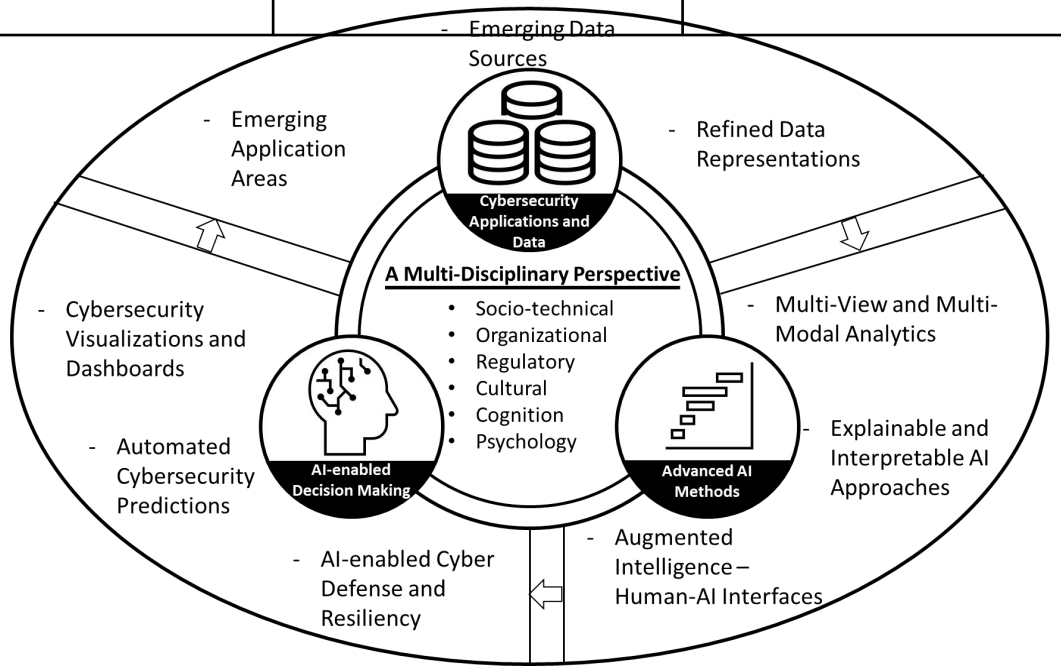
- **Characteristics of External (outside of an organization) Data:**
  - Gives a perspective of threats external to an organization.
  - Primarily generated by humans high velocity, non-standard formats with significant noise.
  - Often less included when teaching AI for cybersecurity.

Existing AI for Cybersecurity Initiatives

Initiative	Selected Common Tasks	Selected Datasets	Selected Software	Sample Conferences
Cyber Threat Intelligence	Malware analysis	VirusTotal	Cuckoo	CAMLIS, IEEE ISI, ASONAM, IEEE DLS, ACM AISec
	Phishing detection	PhishTank	PhishMonger	
	Dark Web Analysis	AZSecure HAP	ISILinux	
Disinformation and Computational Propaganda	Bot detection	Bot Repo, Twitter Bot-Cyborg	Hoaxy, Botometer	IEEE ISI
	Disinformation identification	Credibility Coalition, GOP Twitter	Exifdata, exiftool, factcheck	MisInfoCon
Security Operations Centers	Log file analysis	Boss of the SOC, OmniSOC	Kiwi, Splunk	IEEE VizSec, NDSS, AI Village, IEEE DLS, ACM AISec
	Vulnerability assessment	NVD, Metasploit, ResearchSOC	Nessus, Zmap, OpenVAS	
	Intrusion detection	KDD 1999	Zeek	
Adversarial ML to Robustify Cyber-defenses	Malware evasion, Phishing evasion	EMBER, NIPS Adverarial learning	EvadeML, SecML, EMBER	IEEE DLS, ScAINet, AI Village

- **Key Limitations:**
  1. Often siloed resources and initiatives between academia and industry.
  2. Lack of publicly accessible and realistic datasets.
  3. Model sharing and software sharing remains a challenge.

Education and Research Opportunities…



Outline

- My Background
- Objective and Disclaimers
- An Overview of AI for Cybersecurity
- Sample AI for Cybersecurity Research Illustration
- Workforce Development, Archival Mechanisms, and Funding Opportunities
- Conclusion

Existing AI for Cybersecurity Initiatives

Initiative	Selected Common Tasks	Selected Datasets	Selected Software	Sample Conferences
CTI	Malware analysis	VirusTotal	Cuckoo	CAMLIS, IEEE ISI, ASONAM, IEEE DLS, ACM AISec
	Phishing detection	PhishTank	PhishMonger	
	Dark Web Analysis	AZSecure HAP	ISILinux	
Disinfo. and Comp. Propaganda	Bot detection	Bot Repo, Twitter Bot-Cyborg	Hoaxy, Botometer	IEEE ISI
	Disinformation identification	Credibility Coalition, GOP Twitter	Exifdata, exiftool, factcheck	MisInfoCon
SOC	Log file analysis	Boss of the SOC	Kiwi, Splunk	IEEE VizSec, NDSS, AI Village, IEEE DLS, ACM AISec
	Vuln. assessment	NVD, Metasploit	Nessus, Zmap, OpenVAS	
	Intrusion detection	KDD 1999	Zeek	
Adversarial ML to Robustify CD	Malware/phishing evasion	EMBER, NIPS Adv. learning	EvadeML, SecML	IEEE DLS, ScAINet, AI Village

- **Key Limitations:**
  1. Often siloed resources and initiatives.
  2. Lack of publicly accessible and realistic datasets.
  3. Model sharing and software sharing remains a challenge.

Dark Web Analytics: *"Know your enemy"*

Vulnerability Assessment: *"Know your weaknesses"*

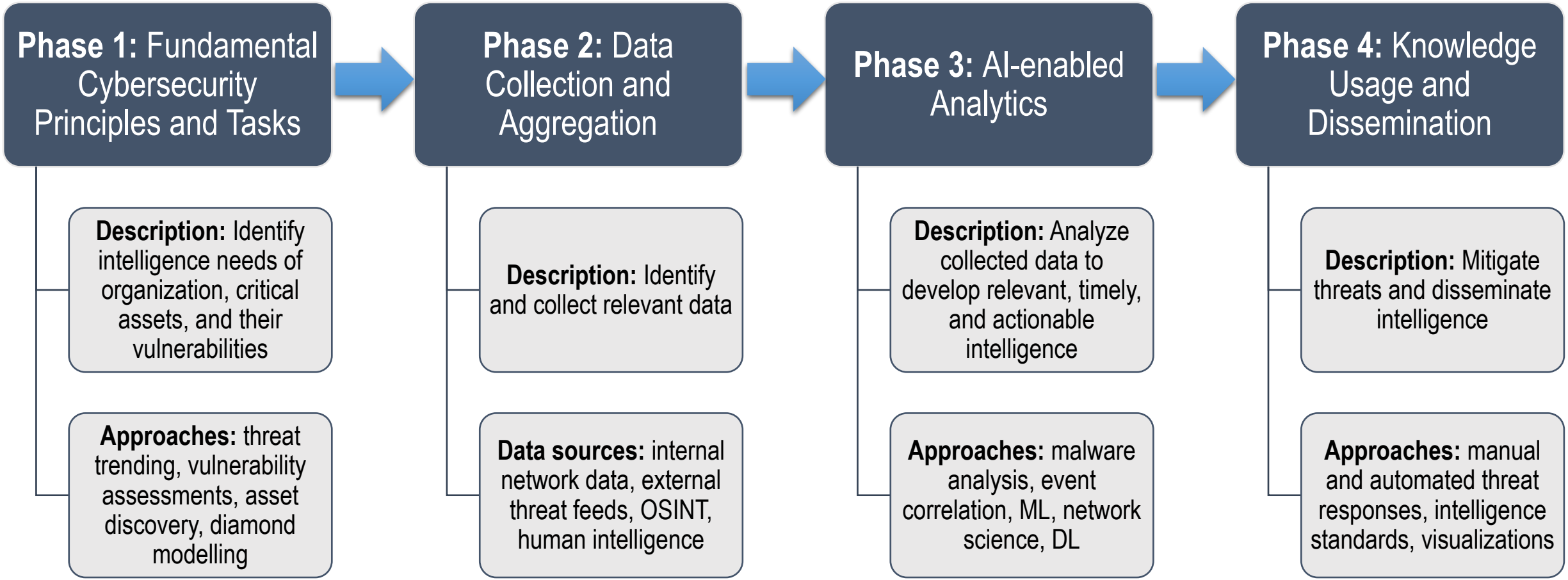
- **Potential Value of AI for Cybersecurity on OmniSOC Data:**
  - How can the exploits from the Dark Web be linked with known vulnerabilities of devices?
  - How can devices be prioritized based on their vulnerabilities and exploits targeting them?
- **Value → holistic, proactive cyber threat intelligence (CTI).**

Dark Web Forum Analysis – Past Literature

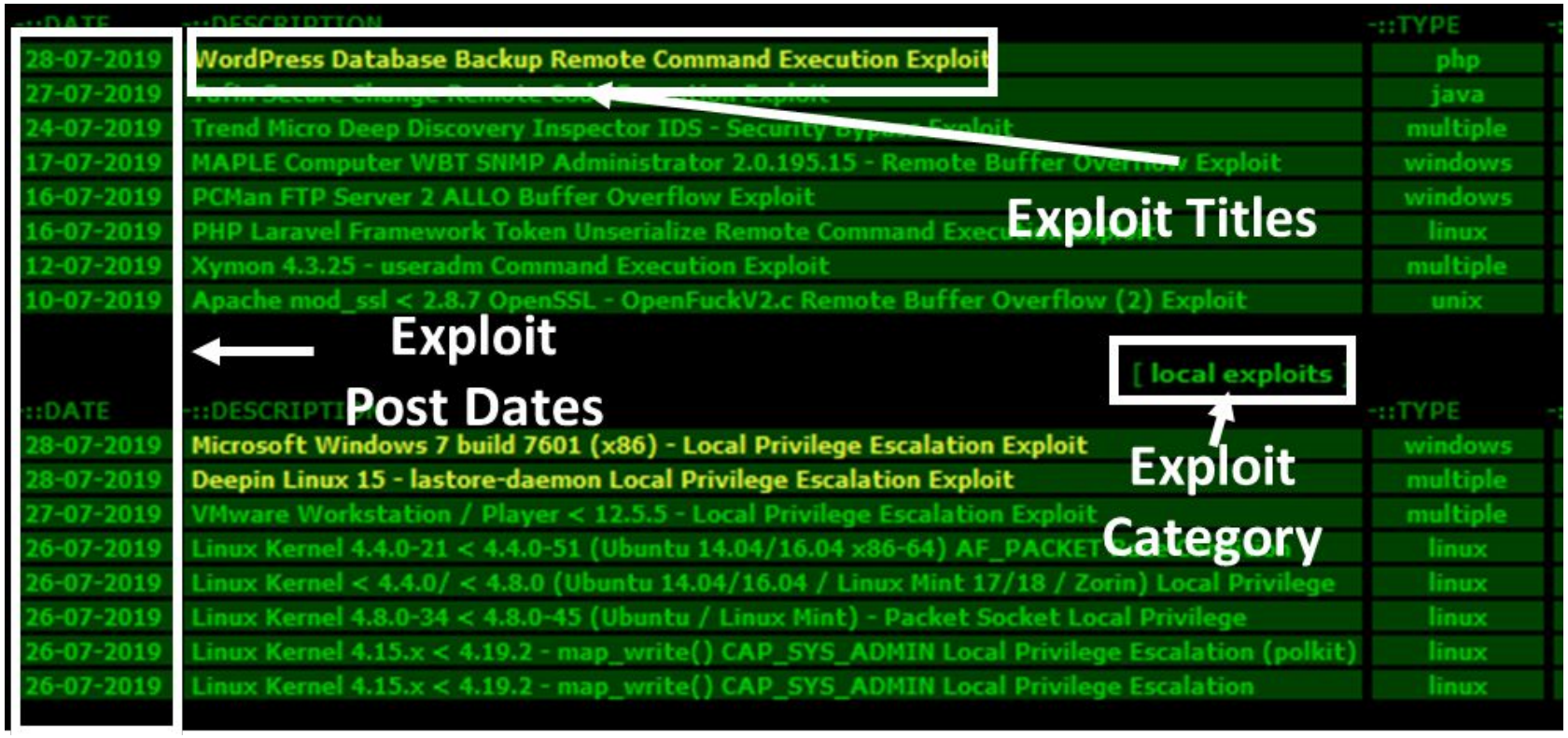
Year	Author	Forum Type 1.	CTI Task(s)	Methods 2.	Identified Exploits* 3.
2019	Schäfer et al.	Seven general purpose	Forum exploration and categorization	Network analysis	DDoS, botnets, DoS
2019	Benjamin et al.	Four general purpose	Hacker reputation	OLS Regression	Rootkit, DDoS, XSS, SQli
2018	Deliu et al.	One general purpose	Exploit categorization	SVM, LDA	Botnet, crypter, DDoS, rootkit
2018	Deliu et al.	One general purpose	Exploit categorization	SVM, CNN	Spamming, crypters, SQLi
2018	Williams et al.	10 general purpose	Incremental collection and categorization	LSTM	Database, network, mobile, system
2017	Sapienza et al.	200 forums and markets	Identifying emerging trends	Keywords	Botnets, DDoS, DoS
2017	Samtani et al.	Five general purpose	Exploit categorization, key hacker ID,	SVM, LDA, SNA	Bots, crypters, keyloggers, phishing, SQLi
2017	Grisham et al.	Four general purpose	Detecting emerging mobile malware	RNN, SNA	Mobile malware
2016	Samtani and Chen	Seven general purpose	Identifying key hackers	SNA	Keyloggers
2016	Li et al.	Three carding forums	Exploring hacker exploits	sLDA	Malware, phishing, botnets
2016	Nunes et al.	12 general purpose	Exploring hacker exploits	SVM	Botnets, keyloggers, worms, 0-days
2015	Samtani et al.	Five general purpose	Exploring hacker exploits	SVM, LDA	Bots, crypters, web exploits, password
2014	Hutchings and Holt	13 general purpose	Exploring hacker exploits	Manual	Keyloggers, phishing, banking Trojans
2014	Ablon et al.	Black markets	Exploring hacker exploits	SME interviews	Payloads, full services
2013	Sood and Enbody	General purpose	Exploring hacker exploits	Manual	Botnets, phishing

- **Key Observations and Gaps:**
  1. Significant focus on collecting, exploring, and categorizing exploits.
  2. Methods were conventionally manual; has evolved to ML and DL techniques.
  3. Lack of work identifying how exploits relate to an organization's vulnerabilities.

AI for Cybersecurity – A General Approach



Hacker Forum Exploit Data Characteristics

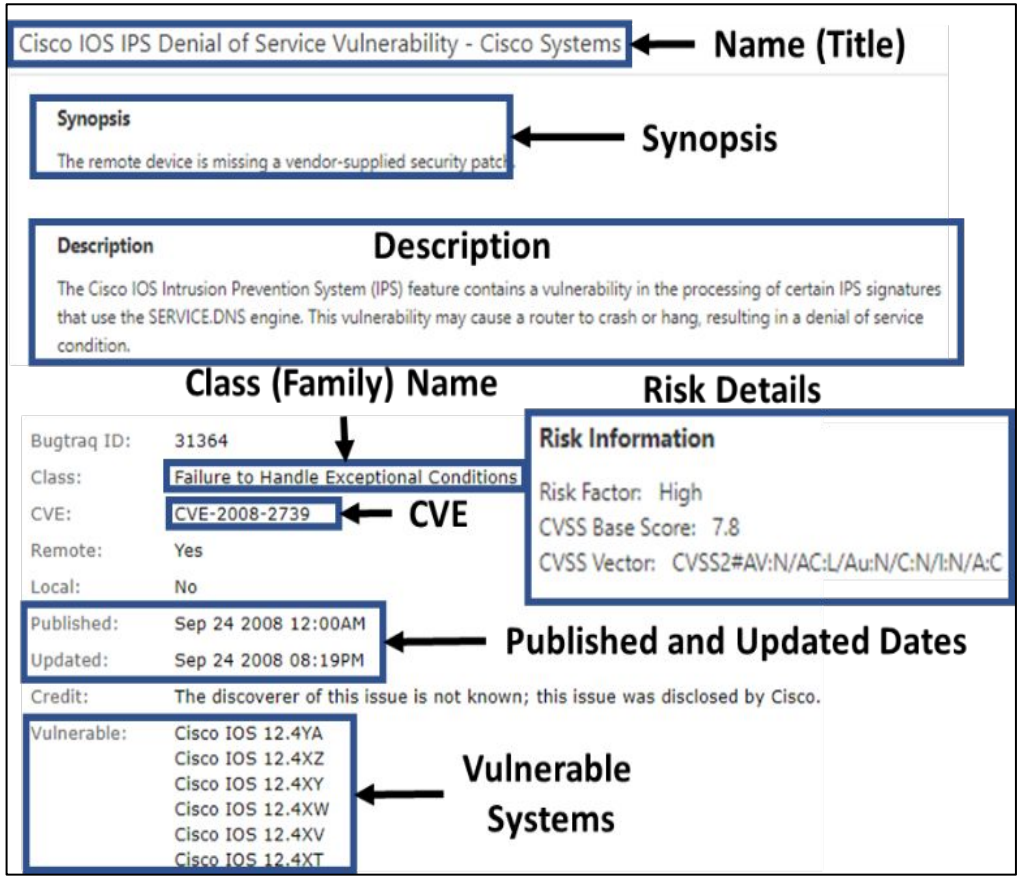


::DATE	::DESCRIPTION	::TYPE
28-07-2019	WordPress Database Backup Remote Command Execution Exploit	php
27-07-2019	[illegible]	java
24-07-2019	Trend Micro Deep Discovery Inspector IDS - Security [illegible] Exploit	multiple
17-07-2019	MAPLE Computer WBT SNMP Administrator 2.0.195.15 - Remote Buffer Overflow Exploit	windows
16-07-2019	PCMan FTP Server 2 ALLO Buffer Overflow Exploit	windows
16-07-2019	PHP Laravel Framework Token Unserialize Remote Command Execution Exploit	linux
12-07-2019	Xymon 4.3.25 - useradm Command Execution Exploit	multiple
10-07-2019	Apache mod_ssl < 2.8.7 OpenSSL - OpenFuckV2.c Remote Buffer Overflow (2) Exploit	unix

::DATE	::DESCRIPTION	::TYPE
28-07-2019	Microsoft Windows 7 build 7601 (x86) - Local Privilege Escalation Exploit	windows
28-07-2019	Deepin Linux 15 - lastore-daemon Local Privilege Escalation Exploit	multiple
27-07-2019	VMware Workstation / Player < 12.5.5 - Local Privilege Escalation Exploit	multiple
26-07-2019	Linux Kernel 4.4.0-21 < 4.4.0-51 (Ubuntu 14.04/16.04 x86-64) AF_PACKET [illegible]	linux
26-07-2019	Linux Kernel < 4.4.0/ < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18 / Zorin) Local Privilege	linux
26-07-2019	Linux Kernel 4.8.0-34 < 4.8.0-45 (Ubuntu / Linux Mint) - Packet Socket Local Privilege	linux
26-07-2019	Linux Kernel 4.15.x < 4.19.2 - map_write() CAP_SYS_ADMIN Local Privilege Escalation (polkit)	linux
26-07-2019	Linux Kernel 4.15.x < 4.19.2 - map_write() CAP_SYS_ADMIN Local Privilege Escalation	linux

- **Key Characteristics:**
  1. Descriptive tool names (target, operations, version names, etc.)
  2. Clear categories of exploits (e.g., target system)
  3. Post date of when exploit was posted

Vulnerability Assessment Data Characteristics



BURPSUITE PROFESSIONAL

Nessus

OpenVAS
Open Vulnerability Assessment Scanner

Category	Metadata	Description	Data Type
Description	Name	Short, descriptive name of vulnerability	Short text
1.	Family Name	Family vulnerability belongs to (e.g., Windows, etc.)	Categorical
	Description	Lengthy text description about vulnerability	Long text
	Synopsis	Short description of vulnerability	Short text
	Solution	Description or solution links	Short text
2.	Vulnerable Systems	List of systems susceptible to vulnerability	Short text (list)
Risk	CVSS	Value between 0.0-10.0 indicating vulnerability severity	Continuous
3.	Risk Factor	Categorical rating of risk (High, Low)	Categorical
	CVE	Vulnerability reference number	Categorical
	Publication Date	Date vulnerability was publicly published	Date

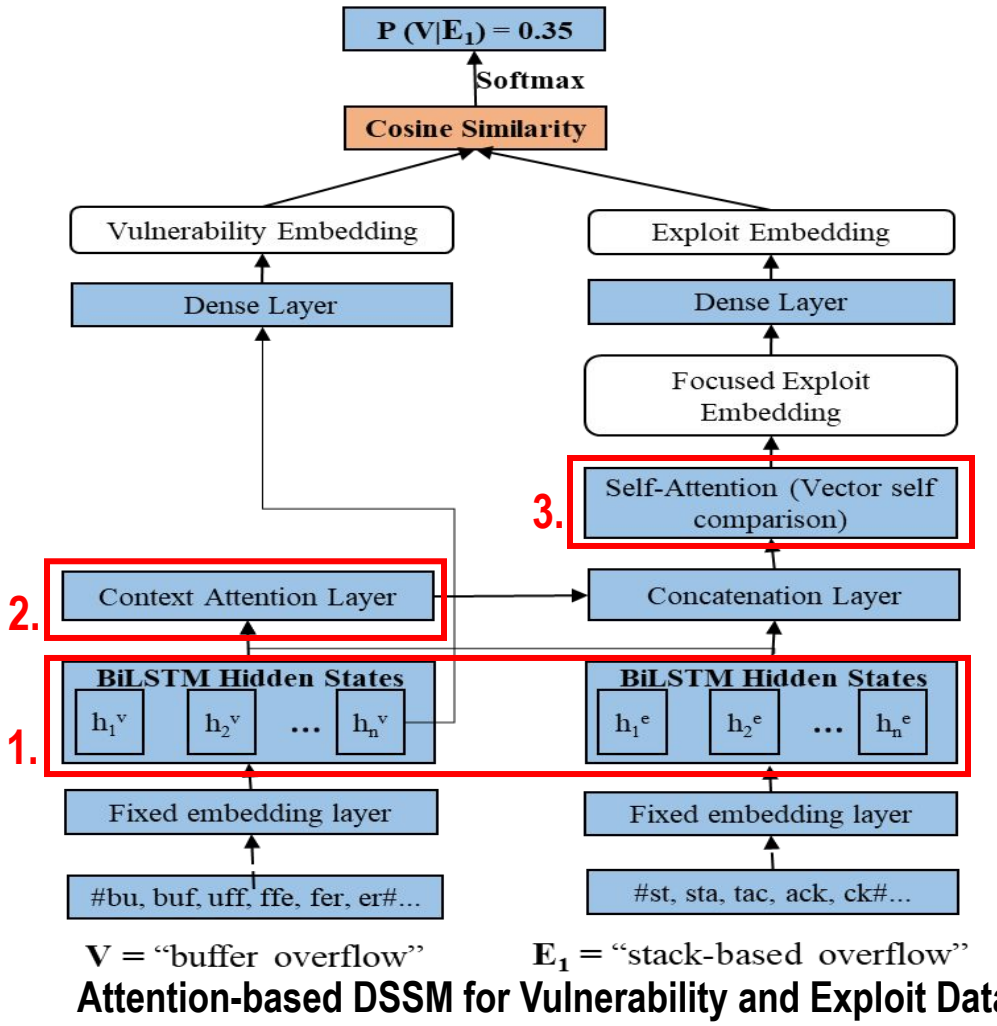
Key Attributes Returned by Modern Vulnerability Scanners

- **Key Characteristics:**
  1. Short, descriptive title of vulnerability
  2. List of systems susceptible to vulnerability
  3. Common Vulnerability Severity Score (0.0 – 10.0)

Sample AI for Cybersecurity Project – Linking Vulnerabilities to Exploits

- **Objective:** Link exploits and vulnerabilities based on their short text similarities names with a novel attention-based DSSM.

- **The Attention-based DSSM's design novelties include:**
  1. Replaces DSSM's bag of letter trigrams approach with a BiLSTM layer to capture sequential dependencies.
  2. Incorporates a novel context attention layer to capture global dependencies across exploit and vulnerability names.
  3. Incorporates a self-attention to identify highest weighted letter trigrams across input texts (to support interpretability).



Attention-based DSSM for Vulnerability and Exploit Data

DVSM Formulation – Linking Exploit and Vulnerability Metadata

- Formally, the DVSM is denoted as:

- **One possible formulation**
- **Customizable to an organization's needs**

- Where:
  - D is the overall device severity score
  - s_j represents the severity of a vulnerability within the device
  - d_j is the # of days since the most relevant exploit for the vulnerability s_j was posted (end date is 6/1/2017), creating a decaying effect of the inverse log function
  - +2 offset prevents DVSM from becoming undefined

- Intuitively, a device's score is higher if it has more vulnerabilities and/or recent exploits.

Hospital Case Study

Hospital Device Information		Device Severity Score Information for Selected Devices			
Hospital Name	**# of Vulnerable Devices/# of devices**	**Device Type**	**# of Vulnerabilities**	**Vulnerabilities**	**DVSM**
12x.x.x.x	133/808	FTP/SSH Server	3	FTP issues	4.591
19x.x.x.x	27/301	SSH Server	3	SSH issues	4.376
17x.x.x.x	31/274	eCare web portal	47	XSS, OpenSSL, buffer overflow, DoS	61.761
16x.x.x.x	59/160	Medical computing portal	5	PHP and SSH issues	4.863
14x.x.x.x	64/130	Web Server	3	SQL Injections	7.528
		Apple TV	2	Buffer overflow	5.381
14x.x.x.x	14/107	SSH/Web server	4	PHP and SSH issues	3.871
6x.x.x.x	9/52	Informational diabetes portal	3	SVN and Unix vulnerabilities	7.159
16x.x.x.x	7/47	Web Server	6	XSS, HTMLi	9.367
Total:	**344/1,879 (18.31%)**	-	-	-	-

Vulnerability Name (CVSS Score)	Exploit Name (Post Date)	Severity Score
"OpenSSL Unsupported" (10.0)	*"OpenSSL TLS Heartbeat Extension – Memory Disclo..."* (4/8/2014)	3.366
"Multiple XSS Vulnerabilities" (4.3)	*"Portal XSS Vulnerability"* (5/28/2010)	1.261
...	...	...
-	-	**Total: 61.761**

- Portals are a common avenue for hackers to access sensitive records.
- Analysis shows an eCare portal with a large attack surface: 47 vulnerabilities for a DVSM of 61.761.
- Network admins can prioritize this device when analyzing their weaknesses.

Outline

- My Background
- Objective and Disclaimers
- An Overview of AI for Cybersecurity
- Sample AI for Cybersecurity Research Illustration
- Workforce Development, Archival Mechanisms, and Funding Opportunities
- Conclusion

Cultivating the AI for Cybersecurity Discipline

- Cultivating the AI for Cybersecurity discipline could potentially be done with a combination of three perspectives:

1. **Workforce Development:** how to cultivate the next generation of Cyber-AI professionals?
2. **Publication (Archival) Opportunities:** how to archive and store knowledge contributions (research)?
3. **Funding Opportunities:** how to support systematic research and education programs?

How to Cultivate the "Cyber AI" Workforce?

Workforce Development: how to cultivate the next generation of Cyber-AI professionals?

Level	Idea	Example (High-Level) Outcomes
Local	Surveying the recruitment pipeline	Identifying URMs, systematic K-12 outreach
	Identify data sources in each program	Targeted recommendation of AI content
	Increased lab resources and prof. development funds	Increased Cyber AI infrastructure literacy
Regional (State or Geographic)	Regional AI for cybersecurity conferences and meet-ups	Localized recruitment and job placement
	Regional AI for cybersecurity ranges and infrastructures	Enhanced collabs; local curricular innovations
National	Survey the government for AI for cybersecurity needs	Identifying job positions, titles, and skills
	Engagement with academic and practitioner venues	Enhanced networking; identifying relevant topics
	Increased calls for dataset and tool sharing	Increased data and model sharing;

Selected Publication (Archival) Opportunities

Publication (Archival) Opportunities: how to archive and store knowledge contributions (research)?

Conference Type	Selected Venue	Relevant Workshop
Academic Security Venues	IEEE S&P	Deep Learning for Security
	ACM CCS	AI for Security
	USENIX	Security and AI Networking Summit
	IEEE ISI	-
Practitioner Security Venues	Cyber Defense	-
	DEFCON	AI Village
	CAMLIS	-
Computer Science AI Venues	ACM KDD	AI-enabled Cybersecurity Analytics
	ASONAM	Foundations of Open Source Intelligence and Security Informatics
	NeurIPS	Trustworthy Machine Learning
	IEEE ICDM	Deep Learning for Cyber Threat Intelligence
NSF Meetings	SaTC PI Meeting	AI for Cyber
	Trusted CI Meeting	-
	SFS Job Fair	-

Selected Funding Opportunities

- **Funding Opportunities:** how to support systematic research and education programs?
- In April 2020, the NSF released a Dear Colleague Letter (DCL) requesting project concepts for "Cybersecurity Education in the Age of Artificial Intelligence."
  - Through the Secure and Trustworthy Cyberspace (SaTC) and Scholarship-for-Service (SFS) programs.
  - Two rounds of submission; 5/15 and 8/31; 30+ concepts **(out of 400+)** were invited for full proposals.

NSF 20-072

Dear Colleague Letter: Cybersecurity Education in the Age of Artificial Intelligence

April 6, 2020

Dear Colleagues:

The National Science Foundation (NSF) is announcing its intention to fund a small number of Early Concept Grants for Exploratory Research (EAGER) to encourage advances in cybersecurity education, an area supported by the Foundation's Secure and Trustworthy Cyberspace Education Designation (SaTC-EDU), CyberCorps®: Scholarships for Service, and Advanced Technological Education (ATE) programs

EAGER is a mechanism to support exploratory work, in its early stages, on untested but potentially transformative research ideas or approaches. This work may be considered especially "high risk – high payoff" in the sense that it, for example, involves radically different approaches, applies new expertise, or engages novel disciplinary or interdisciplinary perspectives.

Selected Funding Opportunities (NSF)

Funding Type	Selected Funding Opportunity*	Funding Ranges
Early Career	CISE Research Initiation Initiative	Up to $175K
	CAREER	Up to $500K
	Presidential CAREER	Up to $500K
Infrastructure Oriented	Cyberinfrastructure for Sustained Scientific Innovation	$200K - $1M
	CISE Community Research Infrastructure	Up to $1.2M
Core Research	SaTC CORE	$500K – $1.2M
	Cybersecurity Innovation for Cyberinfrastructure	$500K – $1M
	Disrupting Illicit Supply Networks	$250K – $1M
Transition to Practice	SaTC Transition to Practice	$500K – $1.2M
	SBIR/STTR	Up to $1.75M of seed funding
	Convergence Accelerator	$3M – $5M
Education Oriented	Scholarship-for-Service	Varies
	SaTC-EDU	Up to $500K
	EAGER AI4Cyber	Up to $300K

*Note: CISE = Computer and Information Sciences and Engineering; EAGER = Early-Concept Grants for Exploratory Research; SaTC = Secure and Trustworthy Cyberspace; SaTC-EDU = SaTC Education; SBIR = Small Business Innovation Research Program; STTR = Small Business Technology Transfer Program.

Outline

- My Background
- Objective and Disclaimers
- An Overview of AI for Cybersecurity
- Sample AI for Cybersecurity Research Illustration
- Workforce Development, Archival Mechanisms, and Funding Opportunities
- Conclusion

Conclusion

- AI and cybersecurity have emerged as critical national priorities.
- Role of AI in cybersecurity help automate prevailing cybersecurity tasks; detect patterns missed by conventional analysis.
- Despite important progress thus far, there remains siloed initiatives, lack of model and data sharing, and other issues.
- Significant opportunity remains to cultivate the next generation of AI for Cybersecurity.

Thank you!

Questions or Comments?

—
Sagar Samtani, Ph.D.
Kelley School of Business, Indiana University
ssamtani@iu.edu
www.sagarsamtani.com

References

1. Anne Johnson and Emily Grumbling (Eds.). 2019. Implications of Artificial Intelligence for Cybersecurity. National Academies Press, Washington, DC. DOI: https://doi.org/10.17226/25488
2. National Science and Technology Council. 2019. The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update. Washington, DC. Retrieved from https://www.nitrd.gov/pubs/National- AI- RD- Strategy- 2019.pdf.
3. National Science Foundation. 2019. National Artificial Intelligence (AI) Research Institutes (2019). nsf20503 | NSF –National Science Foundation. Retrieved from https://www.nsf.gov/pubs/2020/nsf20503/nsf20503.pdf.
4. Sagar Samtani, Murat Kantarcioglu, and Hsinchun Chen. 2020. Trailblazing the Artificial Intelligence for Cybersecurity Discipline. ACM Trans. Manag. Inf. Syst. 11, 4 (December 2020), 1–19. DOI:https://doi.org/10.1145/3430360