Negative: Cybersecurity for the Federal Govt.

By “Coach Vance” Trefethen

***Resolved: The United States federal government should substantially reform the use of Artificial Intelligence technology***

Case Summary: The AFF plan has the federal government contract out new cybersecurity arrangements for government agencies, all of which must use AI. They may also mention a system called “Mayhem,” which was demonstrated in a “Cyber Grand Challenge” competition of hackers trying to prove the value of their systems (although we don’t think their plan actually fiats the government has to use Mayhem). The first 8 solvency arguments apply to any AI cybersecurity, while the last 3 are specifically applying to why Mayhem won’t work (and isn’t topical – it’s not AI). You don’t need the last 3 if they don’t mention Mayhem. Scare the daylights out of the Negative team by road-mapping for the judge at the top of the 1nc that you and your partner are going to have either 8 or 11 Solvency arguments and 2 Disads. The “Segal” source may be cited by the AFF in their plan. He lists both pro’s and con’s of AI cybersecurity in his article, so it’s fair for both sides to be quoting him.

Negative: Cybersecurity for the Federal Government 3

SOLVENCY 3

1. Wrong solution – Secure authentication is the answer 3

FBI cybersecurity expert says: AI is OK, but the best security is more secure user authentication 3

AI has small benefit but usually it’s too late: By the time you detect bad things with AI, they’ve already happened 3

2. Lack of government staffing and qualifications guarantees failure [even if it’s being contracted out] 4

Government lacks the qualified staff to do it themselves or to manage outside contractors. 4

Big human AI talent deficit blocks them from building it themselves and from buying it from the outside. 4

Why it matters: Most so-called “AI” cybersecurity is phony baloney. If government guys don’t know what they’re doing, they’ll get junk systems 4

3. Contractors are the problem, not the solution 5

Federal contractors selling flawed cybersecurity software and covering it up – that’s the problem in Status Quo. 5

4. More AI breakthroughs needed for real success 5

As of June 2021: AI benefit to cybersecurity is incremental at best. Substantial improvement will require significant new breakthroughs that don’t exist yet 5

AI cybersecurity provides incremental improvement at best. A lot more advances and breakthroughs are still needed 6

Machine Learning (ML) cybersecurity isn’t robust enough yet. It may have incremental benefit but: 1) It’s only part of the answer. 2) It’s not a silver bullet that solves everything 7

5. Neural fuzzing 7

Unless AFF fiats that Microsoft is the only bidder allowed to win contracts, AI will be defeated by hackers using “Neural Fuzzing” vulnerabilities 7

6. Hackers use AI too 8

Hackers will defeat your AI with their AI – and this prevents AI from becoming a mainstream security tool 8

7. New avenues of attack = No Net Benefit to AI 8

AI can improve security but it can also make it easier for bad guys to penetrate systems and cause damage 8

AI cybersecurity can open up new avenues of attack that didn’t exist before 9

8. Real world is different from lab tests 10

AFF’s AI cybersecurity high percentage success studies are meaningless. Machine Learning (ML) is difficult to implement in the real world 10

9. A/T “ ‘Mayhem’ AI security system from Cyber Grand Challenge” – Failure #1 – It’s not AI 11

Maybe some day AI will work for autonomous cybersecurity, but Mayhem isn’t it. Mayhem tool made no use of Machine Learning at Cyber Grand Challenge – and that’s how it did better than the AI contestants 11

10. A/T “ ‘Mayhem’ AI security system from Cyber Grand Challenge” – Failure #2 – Needs skilled people 11

Mayhem won’t solve on its own: Still need human experts (which the government doesn’t have see SOLV-2 argument) 11

11. A/T “Mayhem AI security system from Cyber Grand Challenge” – Failure #3 – Only works for Linux 12

Mayhem tool only works on Linux operating system 12

Massive non-use of Linux in the Federal government for sensitive data. Maybe they will someday, but it will be slow 12

[For non-techies who don’t know:] Linux is an “open source” operating system 12

DISADVANTAGES 13

1. Data losses 13

Link: Massive amounts of data have to be given to make AI learning possible 13

Link: Must use government’s data, or else no security advantage. Training on the contractor’s data won’t detect attacks on real data 13

Link: Data goes to contractors under AFF plan 13

Impact: Turn the harms. Contractors lose government data all the time. Some examples: 13

Office of Personnel Management (OPM) in 2015 13

Customs & Border Patrol 2019 14

2. Federal deficits and economic harm 14

Link: Solvency arguments prove the plan is a waste of money 14

Impact: Every dollar in the plan could have been used to reduce the deficit and reduce harm to the US economy 14

Negative: Cybersecurity for the Federal Government

SOLVENCY

1. Wrong solution – Secure authentication is the answer

FBI cybersecurity expert says: AI is OK, but the best security is more secure user authentication

PYMNTS 2021 (consulting firm that does online security for electronic payments and transfer of money) 8 July 2021 “FBI: Why AI And MFA Provide The Most Effective Fraud Defense” <https://www.pymnts.com/fraud-prevention/2021/fbi-ai-mfa-cybercrime-defense/> (accessed 24 Jan 2022)

“In our collection of cyber fraud investigations that we have within the cyber division of the FBI, [we found that] 99 percent of attacks leveraged compromised username [and] password combinations,” said Alvarez. “This is stuff that they’re finding on the dark web, or [gained from] brute-forcing simple passwords because humans just can’t remember more sophisticated passwords.” Businesses are working on several countermeasures to prevent these attacks as permanent work-from-home operations become more widespread. AI-based systems have their uses, Alvarez said, but the best security systems rely on more secure user authentication.

AI has small benefit but usually it’s too late: By the time you detect bad things with AI, they’ve already happened

PYMNTS 2021 (consulting firm that does online security for electronic payments and transfer of money) 8 July 2021 “FBI: Why AI And MFA Provide The Most Effective Fraud Defense” <https://www.pymnts.com/fraud-prevention/2021/fbi-ai-mfa-cybercrime-defense/> (accessed 24 Jan 2022)

The primary benefit of AI-based systems, according to Alvarez, is that they can detect minute patterns and inconsistencies fraudsters may cause that human analysts might not catch. These analyses are typically only performed while a fraudster is already in the system or has just left it, though, meaning that a reliance on these systems can risk the loss of precious data, even if the fraudster is caught. “You can definitely leverage these sophisticated tools to understand how your enterprise works on a regular day, and then [see when] that weird anomaly starts happening, like sending data to an abnormal IP,” said Alvarez. “But that’s a bad day because that means the intruders have been in the enterprise for a while. It’s a truism in our cyber-intrusion cases that most of the self-reporting we get from the victims is when they see data leaving.” The best way to prevent fraud is by keeping fraudsters from ever entering the system in the first place through ironclad customer and employee authentication.

2. Lack of government staffing and qualifications guarantees failure [even if it’s being contracted out]

Government lacks the qualified staff to do it themselves or to manage outside contractors.

**Trusting outside contractors without qualified government staffing involved fails because 1) the contractors are “self-interested” – they’re out to make money. The government lacks qualified staff to ensure they’re not getting ripped off. 2) Because the government cannot “test claims in a laboratory” to verify what the contractors are selling really works.**

Prof. Ryan Calo 2017. (Associate Professor, University of Washington School of Law; hosted the first White House workshop on artificial intelligence policy, organized AI workshops for the National Science Foundation) Artificial Intelligence Policy: A Primer and Roadmap <https://lawreview.law.ucdavis.edu/issues/51/2/Symposium/51-2_Calo.pdf> (accessed 8 Aug 2021)

The better-grounded observation is that government lacks the requisite expertise to manage society in such a deeply technically-mediated world. Government bodies are slow to hire up and face steep competition from industry. When the state does not have its own experts, it must either rely on the self-interested word of private firms (or their proxies) or experience a paralysis of decision and action that ill-serves innovation. Thus, one overarching policy challenge is how best to introduce expertise about AI and robotics into all branches and levels of government so they can make better decisions with greater confidence. [**END QUOTE**] The solution could involve new advisory bodies, such as an official Federal Advisory Committee on Artificial Intelligence with an existing department or even a standalone Federal Robotics Commission. Or it could involve resuscitating the Office of Technology Assessment, building out the Congressional Research Service, or growing the Office of Science and Technology Policy. Yet another approach involves each branch hiring its own technical staff at every level. [**HE GOES ON TO CONCLUDE IN THE SAME CONTEXT QUOTE:]** The technical knowledge and affordances of the government — from the ability to test claims in a laboratory to a working understanding of AI in lawmakers and the judiciary — will ultimately affect the government’s capacity to generate wise AI policy.

Big human AI talent deficit blocks them from building it themselves and from buying it from the outside.

National Security Commission on Artificial Intelligence 2021 (bipartisan commission of 15 technologists, national security professionals, business executives, and academic leaders) March 2021 “Final Report” <https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf> (accessed 17 June 2021)

The human talent deficit is the government’s most conspicuous AI deficit and the single greatest inhibitor to buying, building, and fielding AI-enabled technologies for national security purposes. This is not a time to add a few new positions in national security departments and agencies for Silicon Valley technologists and call it a day. We need to build entirely new talent pipelines from scratch.

Why it matters: Most so-called “AI” cybersecurity is phony baloney. If government guys don’t know what they’re doing, they’ll get junk systems

Jon Rubin copyright 2021. (Senior Engineer at ThreatWarrior, focuses on the ThreatWarrior machine learning and backend systems. He has been in the network security space for nearly twenty years) “Claims of AI in Cybersecurity Are Highly Exaggerated” <https://threatwarrior.com/claims-ai-cybersecurity/> (accessed 25 Jan 2022)

Get past the marketing hype, and most so-called ‘AI’ cybersecurity platforms are more like Siri than C3PO  
Many marketers slap the letters “AI” on everything. Products that have never functioned as true AI and never will are now proudly proclaiming it. But saying something doesn’t make it true, and not all AI is created equal anyway. User Entity Behavioral Analysis (UEBA) platforms claim to use AI. They track metrics like bits received per second and alert when they go too high or low. Many analytics platforms claim to use AI for malware detection. They watch out for traffic from domain names made up of random letters. AI can technically be defined as any technology that demonstrates intelligence by being aware of its environment and acting to successfully achieve a goal. So, these examples can be called AI. But it’s a stretch, and that type of AI doesn’t pack much of a punch.

3. Contractors are the problem, not the solution

Federal contractors selling flawed cybersecurity software and covering it up – that’s the problem in Status Quo.

**[Cross-Apply under INHERENCY: Status Quo has a new initiative to solve it]**

Carly Page 2021 (journalist) “DOJ will sue federal contractors that hide cyberattacks and breaches” 7 Oct 2021 <https://techcrunch.com/2021/10/07/doj-will-sue-federal-contractors-that-hide-cyberattacks-and-breaches/> (accessed 25 Jan 2022)

The Civil Cyber-Fraud Initiative, introduced by Deputy Attorney General Lisa O. Monaco this week, will leverage the existing False Claims Act (FCA) to “pursue cybersecurity-related fraud by government contractors and grant recipients.” The initiative will hold entities, such as federal contractors or individuals, accountable when they put U.S. cyber infrastructure at risk by knowingly providing flawed cybersecurity products or services, [according to a DOJ press release](https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative). Similarly, government contractors now also face penalties for “violating obligations” to monitor and report cybersecurity incidents and breaches. It’s the latest response by the Biden administration following [a spate of hacks](https://techcrunch.com/2021/02/23/solarwinds-hackers-targeted-nasa-federal-aviation-administration-networks/) targeting federal agencies, including the Treasury, the State Department and Homeland Security. The DOJ later [blamed](https://techcrunch.com/2021/01/05/fbi-nsa-says-hacks-on-us-federal-agencies-likely-russian-in-origin/) hackers working for Russia’s foreign intelligence service, the SVR, for the espionage campaign. The Russian hackers broke into SolarWinds’ network and planted a backdoor in its Orion software, which helps companies monitor their networks and fleets of devices, and pushed it directly to customer networks with a tainted software update. The initiative will help it build “broad resiliency” against [cybersecurity](https://techcrunch.com/tag/cybersecurity/) intrusions across the public sector and will help government efforts to identify, create and publicize patches for vulnerabilities in commonly used products and services, according to the DOJ. It will also help the government reclaim losses from the companies if found to have failed to meet the government’s security standards.

4. More AI breakthroughs needed for real success

As of June 2021: AI benefit to cybersecurity is incremental at best. Substantial improvement will require significant new breakthroughs that don’t exist yet

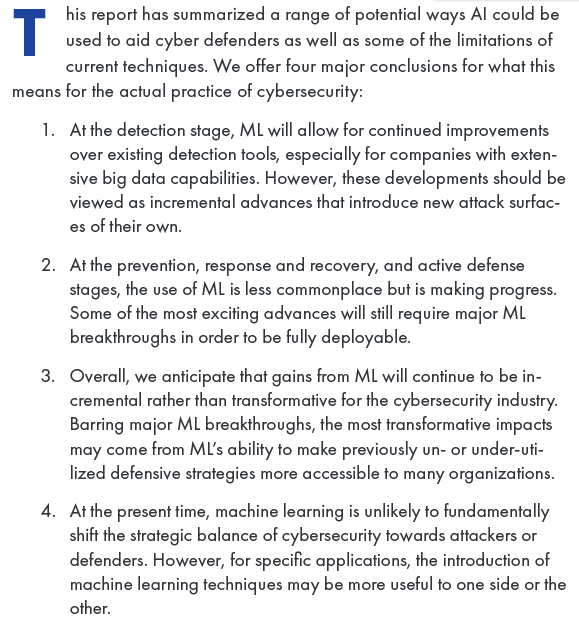
Micah Musser and Ashton Garriott 2021. (Musser - Research Analyst at Georgetown’s Center for Security and Emerging Technology. Garriot - Semester Research Analyst at Georgetown’s Center for Security and Emerging Technology (CSET), where he works on the CyberAI Project. He is a recent graduate of Georgetown’s Security Studies Program ) "Machine Learning and Cybersecurity: Hype and Reality” June 2021 <https://cset.georgetown.edu/publication/machine-learning-and-cybersecurity/> (accessed 26 Jan 2022)

-A wide range of specific tasks could be fully or partially automated with the use of machine learning, including some forms of vulnerability discovery, deception, and attack disruption. But many of the most transformative of these possibilities still require significant machine learning breakthroughs.

-Overall, we anticipate that machine learning will provide incremental advances to cyber defenders, but it is unlikely to fundamentally transform the industry barring additional breakthroughs. Some of the most transformative impacts may come from making previously un- or under-utilized defensive strategies available to more organizations.

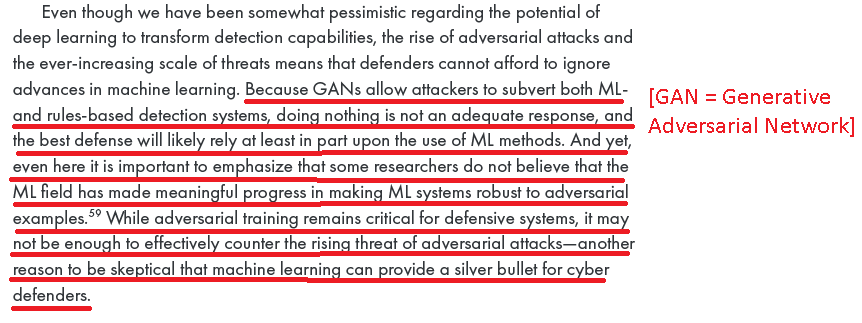
AI cybersecurity provides incremental improvement at best. A lot more advances and breakthroughs are still needed

Micah Musser and Ashton Garriott 2021. (Musser - Research Analyst at Georgetown’s Center for Security and Emerging Technology. Garriot - Semester Research Analyst at Georgetown’s Center for Security and Emerging Technology (CSET), where he works on the CyberAI Project. He is a recent graduate of Georgetown’s Security Studies Program ) "Machine Learning and Cybersecurity: Hype and Reality” June 2021 (brackets added) <https://cset.georgetown.edu/publication/machine-learning-and-cybersecurity/> (accessed 26 Jan 2022)



Machine Learning (ML) cybersecurity isn’t robust enough yet. It may have incremental benefit but: 1) It’s only part of the answer. 2) It’s not a silver bullet that solves everything

Micah Musser and Ashton Garriott 2021. (Musser - Research Analyst at Georgetown’s Center for Security and Emerging Technology. Garriot - Semester Research Analyst at Georgetown’s Center for Security and Emerging Technology (CSET), where he works on the CyberAI Project. He is a recent graduate of Georgetown’s Security Studies Program ) "Machine Learning and Cybersecurity: Hype and Reality” June 2021 (brackets added) <https://cset.georgetown.edu/publication/machine-learning-and-cybersecurity/> (accessed 26 Jan 2022)



5. Neural fuzzing

Unless AFF fiats that Microsoft is the only bidder allowed to win contracts, AI will be defeated by hackers using “Neural Fuzzing” vulnerabilities

Eddie Segal 2020 (*electronics engineer with a Master’s Degree from Be’er Sheva University, a big data and web analytics specialist*) (ethical disclosure: article is undated but internal references to dates, like statistics for the entire year of 2019, show it was written at least in 2020, if not more recently) “The Impact of AI on Cybersecurity” <https://www.computer.org/publications/tech-news/trends/the-impact-of-ai-on-cybersecurity> (accessed 25 Jan 2022)

**Neural fuzzing**—fuzzing is the process of testing large amounts of random input data within software to identify its vulnerabilities. Neural fuzzing leverages AI to quickly test large amounts of random inputs. However, fuzzing has also a constructive side. Hackers can learn about the weaknesses of a target system by gathering information with the power of neural networks. Microsoft [developed a method](https://www.microsoft.com/en-us/research/blog/neural-fuzzing/) to apply this approach to improve their software, resulting in more secure code that is harder to exploit.

6. Hackers use AI too

Hackers will defeat your AI with their AI – and this prevents AI from becoming a mainstream security tool

Eddie Segal 2020 (*electronics engineer with a Master’s Degree from Be’er Sheva University, a big data and web analytics specialist*) (ethical disclosure: article is undated but internal references to dates, like statistics for the entire year of 2019, show it was written at least in 2020, if not more recently) “The Impact of AI on Cybersecurity” <https://www.computer.org/publications/tech-news/trends/the-impact-of-ai-on-cybersecurity> (accessed 25 Jan 2022)

Drawbacks and Limitations of Using AI for Cybersecurity  
There are also some limitations that prevent AI from becoming a mainstream security tool: **[END QUOTE. AND HE GOES ON TO LIST SOME OF THEM, INCLUDING LATER IN THE CONTEXT…]  
Resources**—companies need to invest a lot of time and money in resources like computing power, memory, and data to build and maintain AI systems.  
**Data sets**—AI models are trained with learning data sets. Security teams need to get their hands on many different data sets of malicious codes, malware codes, and anomalies. Some companies just don’t have the resources and time to obtain all of these accurate data sets.

**[QUOTE:]Hackers also use AI**—attackers test and improve their malware to make it resistant to AI-based security tools. Hackers learn from existing AI tools to develop more advanced attacks and attack traditional security systems or even AI-boosted systems.

7. New avenues of attack = No Net Benefit to AI

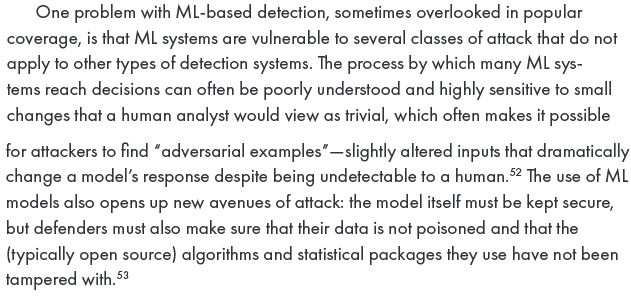
AI can improve security but it can also make it easier for bad guys to penetrate systems and cause damage

Eddie Segal 2020 (*electronics engineer with a Master’s Degree from Be’er Sheva University, a big data and web analytics specialist*) (ethical disclosure: article is undated but internal references to dates, like statistics for the entire year of 2019, show it was written at least in 2020, if not more recently) “The Impact of AI on Cybersecurity” <https://www.computer.org/publications/tech-news/trends/the-impact-of-ai-on-cybersecurity> (accessed 25 Jan 2022)

Conclusion  
Artificial intelligence and machine learning can improve security, while at the same time making it easier for cybercriminals to penetrate systems with no human intervention. This can bring significant damage to any company. Getting some kind of protection against cyber criminals is highly recommended if you want to reduce losses and stay in business.

AI cybersecurity can open up new avenues of attack that didn’t exist before

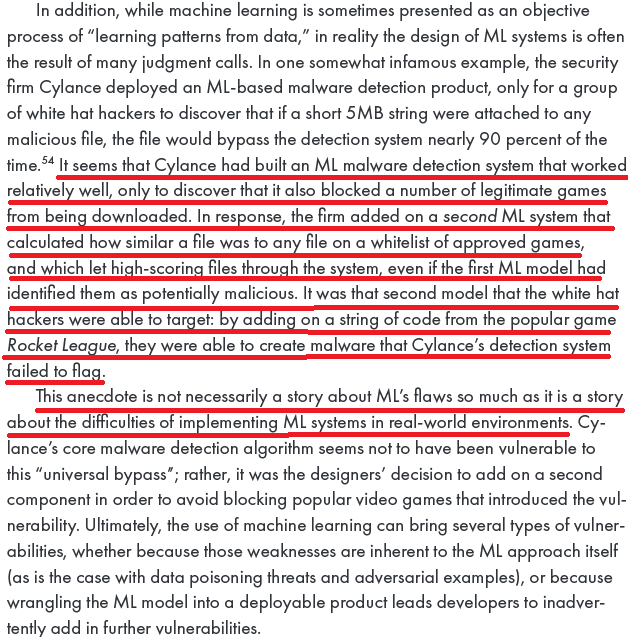
Micah Musser and Ashton Garriott 2021. (Musser - Research Analyst at Georgetown’s Center for Security and Emerging Technology. Garriot - Semester Research Analyst at Georgetown’s Center for Security and Emerging Technology (CSET), where he works on the CyberAI Project. He is a recent graduate of Georgetown’s Security Studies Program ) "Machine Learning and Cybersecurity: Hype and Reality” June 2021 <https://cset.georgetown.edu/publication/machine-learning-and-cybersecurity/> (accessed 26 Jan 2022) (brackets added)



8. Real world is different from lab tests

AFF’s AI cybersecurity high percentage success studies are meaningless. Machine Learning (ML) is difficult to implement in the real world

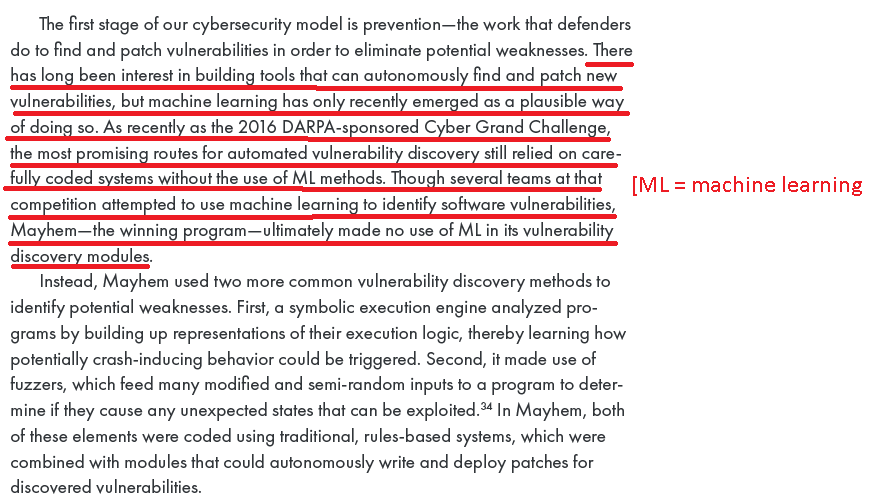
Micah Musser and Ashton Garriott 2021. (Musser - Research Analyst at Georgetown’s Center for Security and Emerging Technology. Garriot - Semester Research Analyst at Georgetown’s Center for Security and Emerging Technology (CSET), where he works on the CyberAI Project. He is a recent graduate of Georgetown’s Security Studies Program ) "Machine Learning and Cybersecurity: Hype and Reality” June 2021 <https://cset.georgetown.edu/publication/machine-learning-and-cybersecurity/> (accessed 26 Jan 2022) (brackets added)



9. A/T “ ‘Mayhem’ AI security system from Cyber Grand Challenge” – Failure #1 – It’s not AI

Maybe some day AI will work for autonomous cybersecurity, but Mayhem isn’t it. Mayhem tool made no use of Machine Learning at Cyber Grand Challenge – and that’s how it did better than the AI contestants

Micah Musser and Ashton Garriott 2021. (Musser - Research Analyst at Georgetown’s Center for Security and Emerging Technology. Garriot - Semester Research Analyst at Georgetown’s Center for Security and Emerging Technology (CSET), where he works on the CyberAI Project. He is a recent graduate of Georgetown’s Security Studies Program ) "Machine Learning and Cybersecurity: Hype and Reality” June 2021 <https://cset.georgetown.edu/publication/machine-learning-and-cybersecurity/> (accessed 26 Jan 2022) (brackets added)



10. A/T “ ‘Mayhem’ AI security system from Cyber Grand Challenge” – Failure #2 – Needs skilled people

Mayhem won’t solve on its own: Still need human experts (which the government doesn’t have see SOLV-2 argument)

Tom Sihonite 2020 (journalist) WIRED 1 June 2020 “This Bot Hunts Software Bugs for the Pentagon” <https://www.wired.com/story/bot-hunts-software-bugs-pentagon/> (accessed 25 Jan 2022)

Mayhem isn’t sophisticated enough to fully replace the work of human bug finders, who use knowledge of software design, code reading skills, creativity, and intuition to find flaws. But ForAllSecure cofounder and CEO David Brumley says the tool can help human experts get more done. The world’s software has more security holes than experts have time to find, and more flaws ship every minute. “Security isn’t about being either secure or insecure, it’s about how fast you can move,” says Brumley.

11. A/T “Mayhem AI security system from Cyber Grand Challenge” – Failure #3 – Only works for Linux

Mayhem tool only works on Linux operating system

Tom Sihonite 2020 (journalist) WIRED 1 June 2020 “This Bot Hunts Software Bugs for the Pentagon” <https://www.wired.com/story/bot-hunts-software-bugs-pentagon/> (accessed 25 Jan 2022)

Brumley says interest from automotive and aerospace companies is particularly strong. [Cars](https://www.wired.com/tag/car-hacking/) and planes [rely increasingly on software](https://www.wired.com/story/boeing-787-code-leak-security-flaws/), which needs to function reliably for years and is [updated rarely](https://www.wired.com/2016/07/chrysler-launches-detroits-first-bug-bounty-hackers/), if at all. Mayhem works only on programs for Linux-based operating systems and finds bugs in two ways, one scattershot, the other more targeted.

Massive non-use of Linux in the Federal government for sensitive data. Maybe they will someday, but it will be slow

Venky Adivi 2021. (journalist) “The stars are aligning for federal IT open source software adoption” <https://techcrunch.com/2021/08/27/the-stars-are-aligning-for-federal-it-open-source-software-adoption/> (accessed 25 Jan 2022)

The federal government has been slower to embrace open source, however. Efforts to change are complicated by the fact that many agencies employ large legacy IT infrastructure and systems to serve millions of people and are responsible for a plethora of sensitive data. Washington spends tens of billions every year on IT, but with each agency essentially acting as its own enterprise, decision-making is far more decentralized than it would be at, say, a large bank. While the government has made a number of moves in a more open direction in recent years, the story of open source in federal IT has often seemed more about potential than reality.

[For non-techies who don’t know:] Linux is an “open source” operating system

Red Hat Software 2019 (vendor of Linux operating system software) 27 Feb 2019 “What is Linux?” <https://www.redhat.com/en/topics/linux/what-is-linux#:~:text=download%20additional%20apps.-,Linux%20and%20open%20source,so%20under%20the%20same%20license>. (accessed 25 Jan 2022)

Linux is a free, open source operating system, released under the [GNU General Public License (GPL)](https://www.redhat.com/en/blog/gpl-cooperation-commitment-and-red-hat-projects). Anyone can run, study, modify, and redistribute the source code, or even sell copies of their modified code, as long as they do so under the same license.

DISADVANTAGES

1. Data losses

Link: Massive amounts of data have to be given to make AI learning possible

Eddie Segal 2020 (*electronics engineer with a Master’s Degree from Be’er Sheva University, a big data and web analytics specialist*) (ethical disclosure: article is undated but internal references to dates, like statistics for the entire year of 2019, show it was written at least in 2020, if not more recently) “The Impact of AI on Cybersecurity” <https://www.computer.org/publications/tech-news/trends/the-impact-of-ai-on-cybersecurity> (accessed 25 Jan 2022)

Drawbacks and Limitations of Using AI for Cybersecurity

There are also some limitations that prevent AI from becoming a mainstream security tool:

**Resources**—companies need to invest a lot of time and money in resources like computing power, memory, and data to build and maintain AI systems.

**Data sets**—AI models are trained with learning data sets. Security teams need to get their hands on many different data sets of malicious codes, malware codes, and anomalies. Some companies just don’t have the resources and time to obtain all of these accurate data sets.

Link: Must use government’s data, or else no security advantage. Training on the contractor’s data won’t detect attacks on real data

Jon Rubin copyright 2021. (Senior Engineer at ThreatWarrior, focuses on the ThreatWarrior machine learning and backend systems. He has been in the network security space for nearly twenty years) “Claims of AI in Cybersecurity Are Highly Exaggerated” <https://threatwarrior.com/claims-ai-cybersecurity/> (accessed 25 Jan 2022)

Software agents running on laptops don’t have much computing power available without impacting the user experience, so it’s generally a one-size-fits-all design. A centralized AI model is trained by the vendor on proprietary data and the result delivered to all the clients. These systems don’t know your environment, so they can’t use context and history to weigh threat severities. They’re not going to detect novel zero-day attacks. They just detect malware using techniques like the ones they trained on, which is only one of the many problems plaguing agent-based solutions.

Link: Data goes to contractors under AFF plan

If the contractors don’t see the data, they can’t build the system.

Impact: Turn the harms. Contractors lose government data all the time. Some examples:

Office of Personnel Management (OPM) in 2015

Aaron Boyd 2015. (journalist) FEDERAL TIMES 23 June 2015 “Contractor breach gave hackers keys to OPM data” <https://www.federaltimes.com/smr/opm-data-breach/2015/06/23/contractor-breach-gave-hackers-keys-to-opm-data/> (accessed 25 Jan 2022)

A breach of KeyPoint Government Solutions — a contractor used by federal agencies to conduct background checks — gave hackers the credentials needed to access sensitive employee data held by the Office of Personnel Management, the agency director confirmed Tuesday. During a hearing in front of the Senate Appropriations Subcommittee on Financial Services and General Government, OPM Director Katherine Archuleta told legislators there was a direct line between the August breach of KeyPoint systems and the two intrusions of OPM servers detected in April.

Customs & Border Patrol 2019

Brian Krebs 2019. (Bachelor of Arts in International Studies; journalist; cybersecurity expert) Secret Service Investigates Breach at U.S. Govt IT Contractor 9 Sept 2019 <https://krebsonsecurity.com/2019/09/secret-service-investigates-breach-at-u-s-govt-it-contractor/> (accessed 25 Jan 2022)

In July, DHS’s Customs and Border Patrol (CPB) [suspended all federal contracts](https://www.washingtonpost.com/technology/2019/07/02/border-surveillance-subcontractor-suspended-after-cyberattack-misuse-traveler-images/?arc404=true) with **Perceptics**, a contractor which sells license-plate scanners and other border control equipment, after data collected by the company was [made available for download on the dark web](https://www.theregister.co.uk/2019/05/23/perceptics_hacked_license_plate_recognition/). The CPB later said the breach was the result of a federal contractor copying data on its corporate network, which was subsequently compromised.

2. Federal deficits and economic harm

Link: Solvency arguments prove the plan is a waste of money

We’d be spending billions on something that adds no value

Impact: Every dollar in the plan could have been used to reduce the deficit and reduce harm to the US economy

Dr William Gale and Benjamin Harris 2010. (Gale - PhD in economics, Stanford Univ.; senior fellow at the Brookings Institution and co-director of the Urban-Brookings Tax Policy Center; former assistant professor of Economics at UCLA, and a senior economist for the Council of Economic Advisers under President George H.W. Bush; Harris - master’s degree in economics from Cornell Univ and master’s degree in quantitative methods from Columbia University; senior research associate with the Economics Studies Program at the Brookings Institution) “A VAT for the United States: Part of the Solution” (notes about the date: This article is one of several in the overall publication at this source. The publication date was 2011, but this article was written in 2010) <https://www.taxpolicycenter.org/sites/default/files/alfresco/publication-pdfs/1001418-A-Value-Added-Tax-for-the-United-States-Part-of-the-Solution.PDF> (accessed 26 Jan 2022)

But even in the absence of a crisis, sustained deficits have deleterious effects, as they translate into lower national savings, higher interest rates, and increased indebtedness to foreign investors, all of which serve to reduce future national income. Gale and Orszag (2004a) estimate that a 1 percent of GDP increase in the deficit will raise interest rates by 25 to 35 basis points and reduce national saving by 0.5 to 0.8 percentage points of GDP.