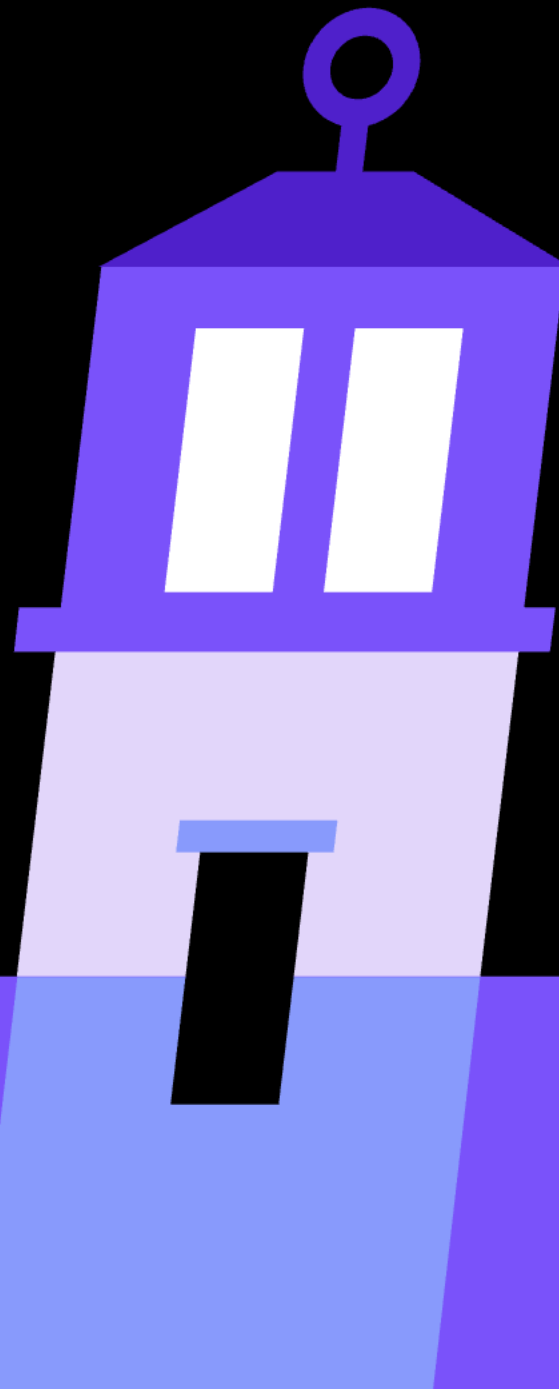




HYBRID
IDENTITY
PROTECTION
conf25





Mind Over Machine: Cyberpsychology of the Human Factor in Hybrid Identity

Dr Mary Aiken, Professor & Chair of Dept of Cyberpsychology
Capitol Technology University Washington D.C.



CYBERPSYCHOLOGY

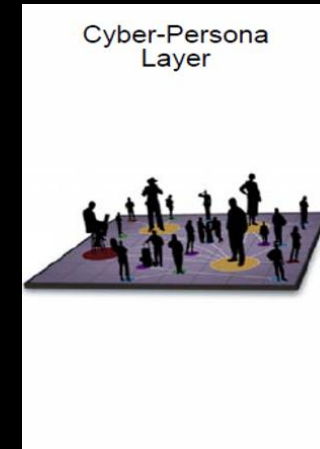
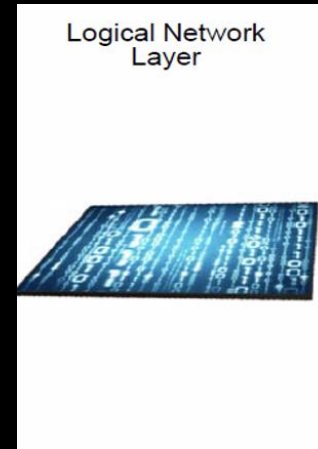
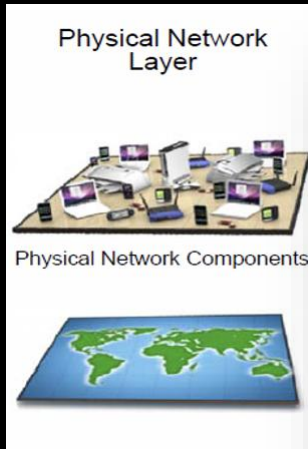


THREE LAYERS OF CYBERSPACE

Cybersecurity

Cyber Safety

Hacktivists & activists
State sponsored actors
State condoned actors
Sophisticated threat actors
Cybercriminals (OCGs)
Targeted Violence
& Terrorism (TVT)
Cyber espionage
Insider threats
Perpetrators of abuse, fraud,
harassment & extortion



HUMANS IN CYBERSPACE

Anonymity (Joinson, 2009)

Online Disinhibition Effect (Suler, 2004)

Online Syndication (Aiken, 2016)

Impulsivity (Aiken et al, 2016)



ONLINE DISINHIBITION



Attacker Behavior:

More aggressive phishing
& impersonation
Manipulative attacks
thrive



User Behavior:

Oversharing/careless
clicks
Reduced caution



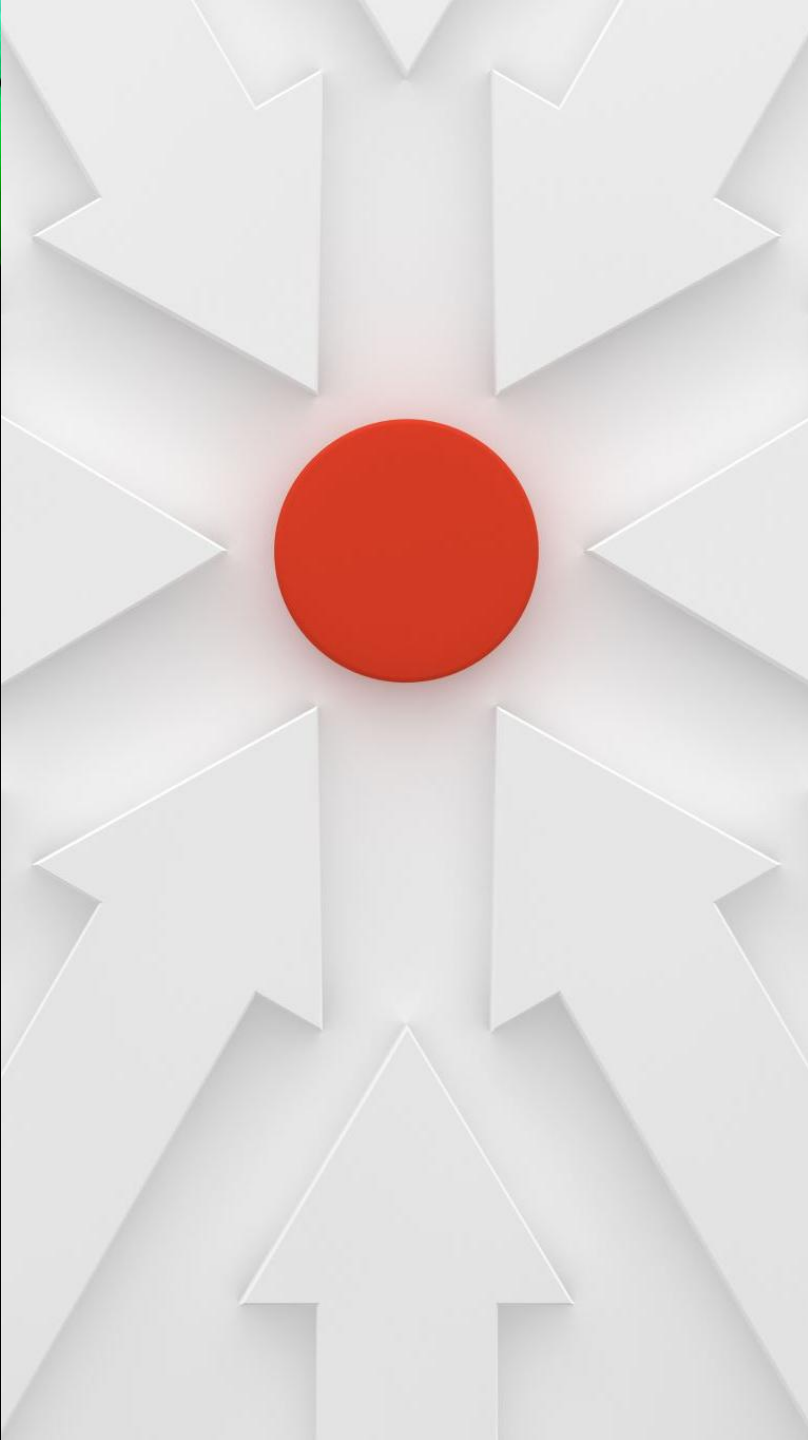
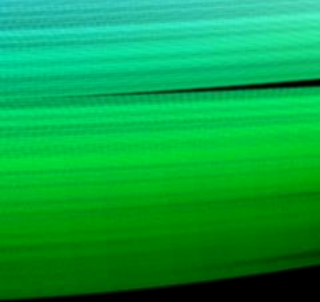
Defense Strategy:

Simulated phishing -
mimics disinhibition triggers
Security nudges &
reminders - critical login
points

HYBRID IDENTITY: CYBERPSYCHOLOGICAL BATTLEFIELD

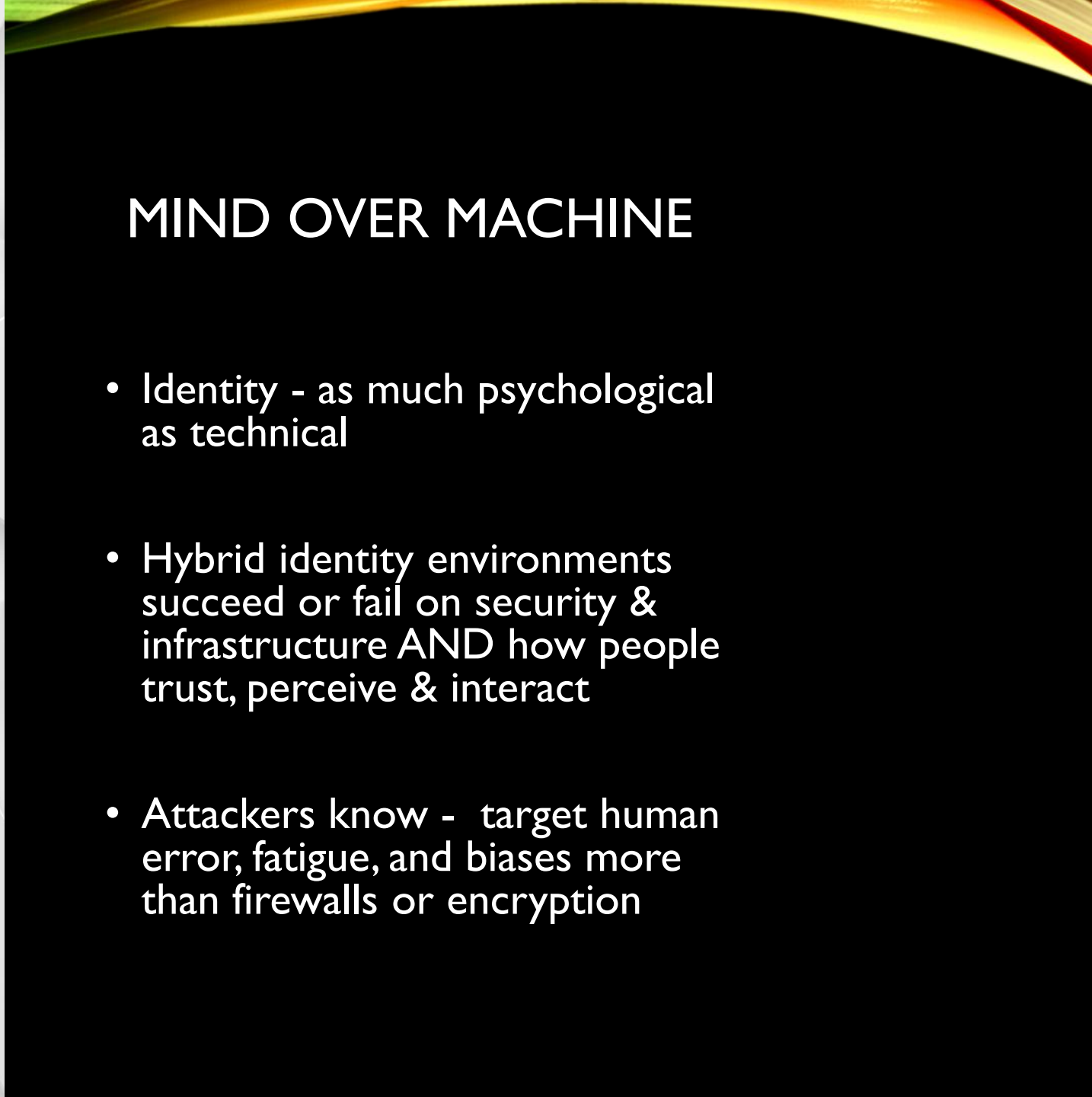
- Attackers weaponize cyberpsychological vulnerabilities
- Users take shortcuts & risks
- Defenders must build psychologically resilient systems
- Trustworthy, transparent, low-friction authentication
- Human-aware defenses



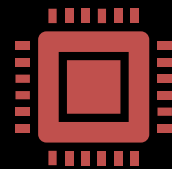


MIND OVER MACHINE

- Identity - as much psychological as technical
- Hybrid identity environments succeed or fail on security & infrastructure AND how people trust, perceive & interact
- Attackers know - target human error, fatigue, and biases more than firewalls or encryption



AI IS CHANGING THE PSYCHOLOGY OF ATTACKS



AI-driven phishing
attacks now
adapt in real time
- feel more
authentic to the
victim

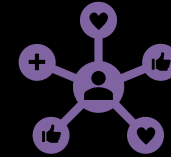


Attacks don't just
trick systems - trick
minds

TRUST & FATIGUE ARE THE NEW BATTLEFIELDS



MFA fatigue
attacks succeed
not because MFA
is weak - but
because humans
are overloaded



Identity defenses
must consider
cognitive load
and security
fatigue

CYBER BEHAVIORAL SCIENCE OFFERS SOLUTIONS



Adaptive
authentication:
fair, transparent &
low-friction
increases
compliance



Training that
addresses
cyberpsychological
triggers (urgency,
authority, fear) more
effective than 'don't
click'



THE FUTURE IS PSYCHOLOGICALLY RESILIENT SYSTEMS

- Success means building systems that people trust, understand & accept culturally - not just technically
- Next-gen identity systems must counter learned helplessness & monitoring anxiety

CYBER BEHAVIORAL ATTACK VECTORS



(I) EXPLOITING COGNITIVE SHORTCUTS

Authority heuristic - when an attacker impersonates

Scarcity/urgency heuristic - “Your account will be locked in 24 hours”

Familiarity heuristic - Fake login portals - users click because it looks right

(2) EXPLOITING COGNITIVE BIASES

Confirmation bias - Users expect MFA push notifications, so they approve them without checking the source (MFA fatigue attacks)

Overconfidence bias - “I’d never fall for phishing” - less vigilance

Automation bias - Blind trust in “secure-looking” login systems or prompts

Availability bias - Recent news of breaches may heighten fear (easy to exploit with fear-based phishing) or desensitize users

(3) EXPLOITING DECISION MAKING UNDER PRESSURE

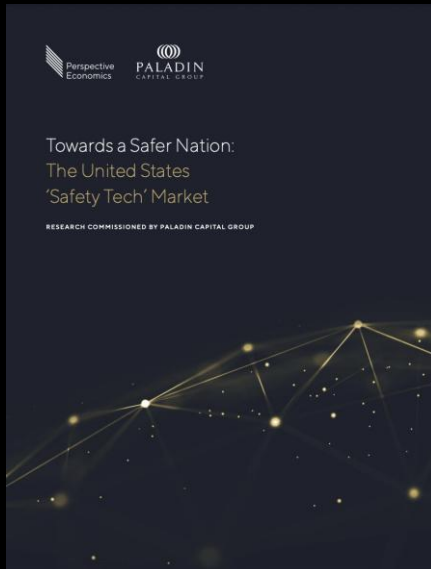
Time pressure - Urgent MFA requests, fake IT helpdesk calls demanding “immediate login”

Information overload - Flooding users with repeated MFA push requests until they approve one

Stress & fatigue – cognitive overload - end-of-day/high-workload phishing attacks when vigilance is lowest

Social pressure - Messages framed as “your boss needs this now” exploit authority + urgency

CYBER SAFETY & “SAFETY TECH”



CYBER
RESILIENCE

&
HUMAN
RESILIENCE



ZERO



TRUST

THE TRUST PARADOX

EVOLVING INSIDER THREATS

Active online recruitment
(OCGs)

“Insider Threat-as-a-Service”
(ITaaS)

Online syndication

Not an anomaly – prototype

Agentic Insiders



FACTORING HUMAN RISK

Employees around the world - hired via Zoom

Pre-Hire Psychometrics

Cyber Psychometric testing & monitoring?



ADVANCED BIOMETRICS

Security Innovation:
Optic Nerve Head
(ONH)



A New Smartphone Optic Nerve Head Biometric for
Verification and Change Detection (Coleman et al, 2021)

IARPA ReSCIND

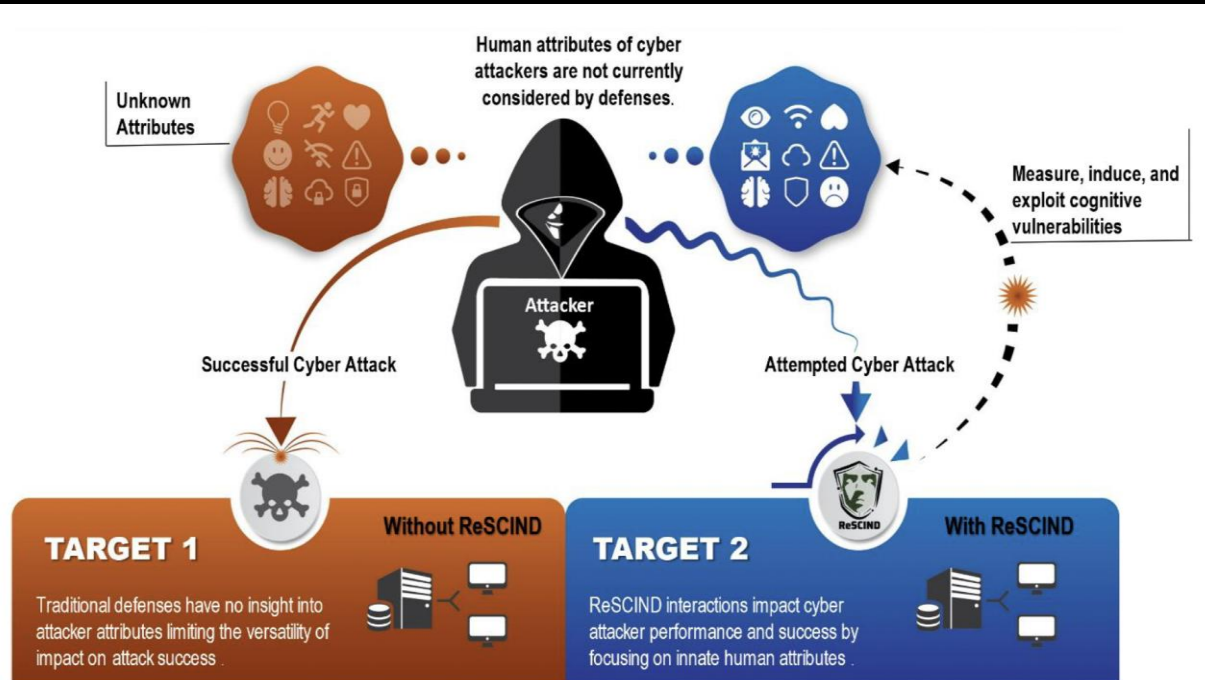


Figure 1: Notional graphic of cyber defense with and without ReSCIND



THE EXPLOIT: WEAPON OF CHOICE

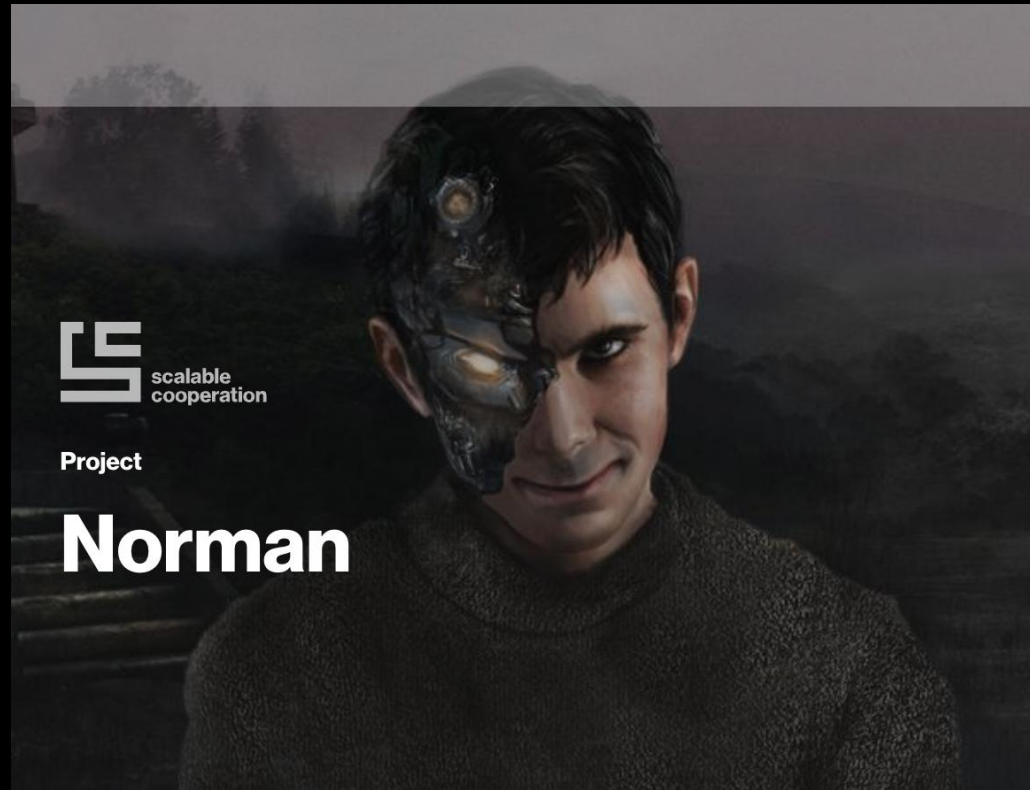


By way of example, Table 1 below lists cyberattacks, hypothetical cyberattacker vulnerabilities, and (subject to testing) programmed HackBot responses.

Cyberattack	Cyberattacker Vulnerability	HackBot Response
Phishing	Need to build trust	Engage & extract intel in trust building exchange - use to counter attack
Malware-Spyware	Paraphilic type state: Voyeurism	Engage & leverage paranoia - imply traceability and attribution
Malware-Ransomware	Dark Tetrad traits	Engage & target impulsivity and need for instant gratification

Table 1. Cyberattack and HackBot response

PSYCHOPATHIC AI



RORSCHACH



PASSIVE DEFENSE

Criminal justice systems
worldwide function on the
premise of consequence,
punishment & deterrence

– Except in Cyberspace



INDUSTRY-LED

Active Cyber Defense



“THE ENTERPRISE STRIKES BACK”

Reversing Social Engineering in the Cyber Defense Context (Lundie et al, 2024)

Cyber defense can no longer be sustained with passive defensive tactics

Industry-wide paradigm shift from passive to active forms of defense “hacking back”

Corporate self-help in cyberspace: contentious issue

Private sector defend their networks –not permitted to retaliate beyond perimeter

Cyberattacker vulnerabilities - targeted and exploited to disrupt cyberattacks

Achieve effective defensive operations without breaching the legal threshold of cyber offensive operations



Q: “AREN’T HYBRID
IDENTITY
ENVIRONMENTS
JUST A TECHNICAL
PROBLEM FOR IT
TEAMS? WHY BRING
PSYCHOLOGY
INTO IT?”

Identity not just about servers and
protocols - it’s about people.



Q: “AI IS
EVERYWHERE RIGHT
NOW. HOW REAL IS
THE THREAT OF AI-
DRIVEN ATTACKS,
OR IS IT JUST HYPE?”

It's not hype - it's happening.

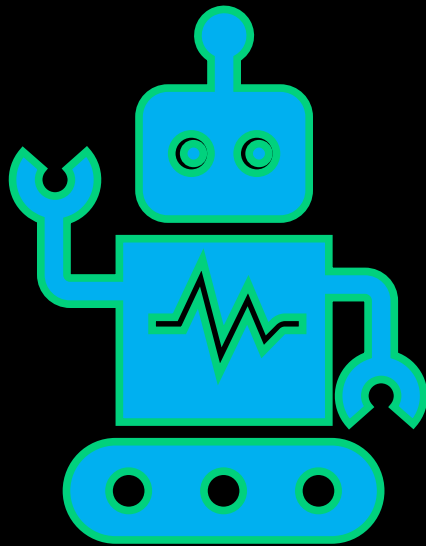


Q: “IF USERS ARE THE
WEAKEST LINK, DOES
THAT MEAN PEOPLE
WILL ALWAYS BE THE
PROBLEM IN
CYBERSECURITY?”

People are not the weakest link –
but the most targeted link.

TAKEAWAYS

AI doesn't just hack machines
it **hacks minds**



Security fatigue - silent
vulnerability in every hybrid
identity environment

Hybrid identity isn't just
technical - it's psychological

CSI:CYBER

The Telegraph

Home Video News World Sport Business Money Com
Film TV and Radio Books Music Comedy Art Theatre
TV Guide TV Reviews BBC Game of Thrones Great British B

HOME » CULTURE » TV AND RADIO

The real-life spook behind CSI: Cyber

Tim Bouquet talks to cyber psychologist Mary Aiken

USA TODAY

A GANNETT COMPANY

NEWS SPORTS LIFE MONEY TECH TRAVEL OPINION 52° CROSSWORDS MORE

Patricia Arquette: From 'Boyhood' to new 'CSI'



IN THE NEWS: MARCH MADNESS TUNISIA ROBERT DURST HILLARY CLINTON

HOME SECTIONS SEARCH

NEW YORK POST

ENTERTAINMENT

Meet Mary Aiken, the inspiration behind 'CSI: Cyber'

By Andrea Morabito March 3, 2015 | 12:25am



Newsweek

HOME WORLD BUSINESS TECH & SCIENCE CULTURE SPORT THIS WEEK'S EDITION

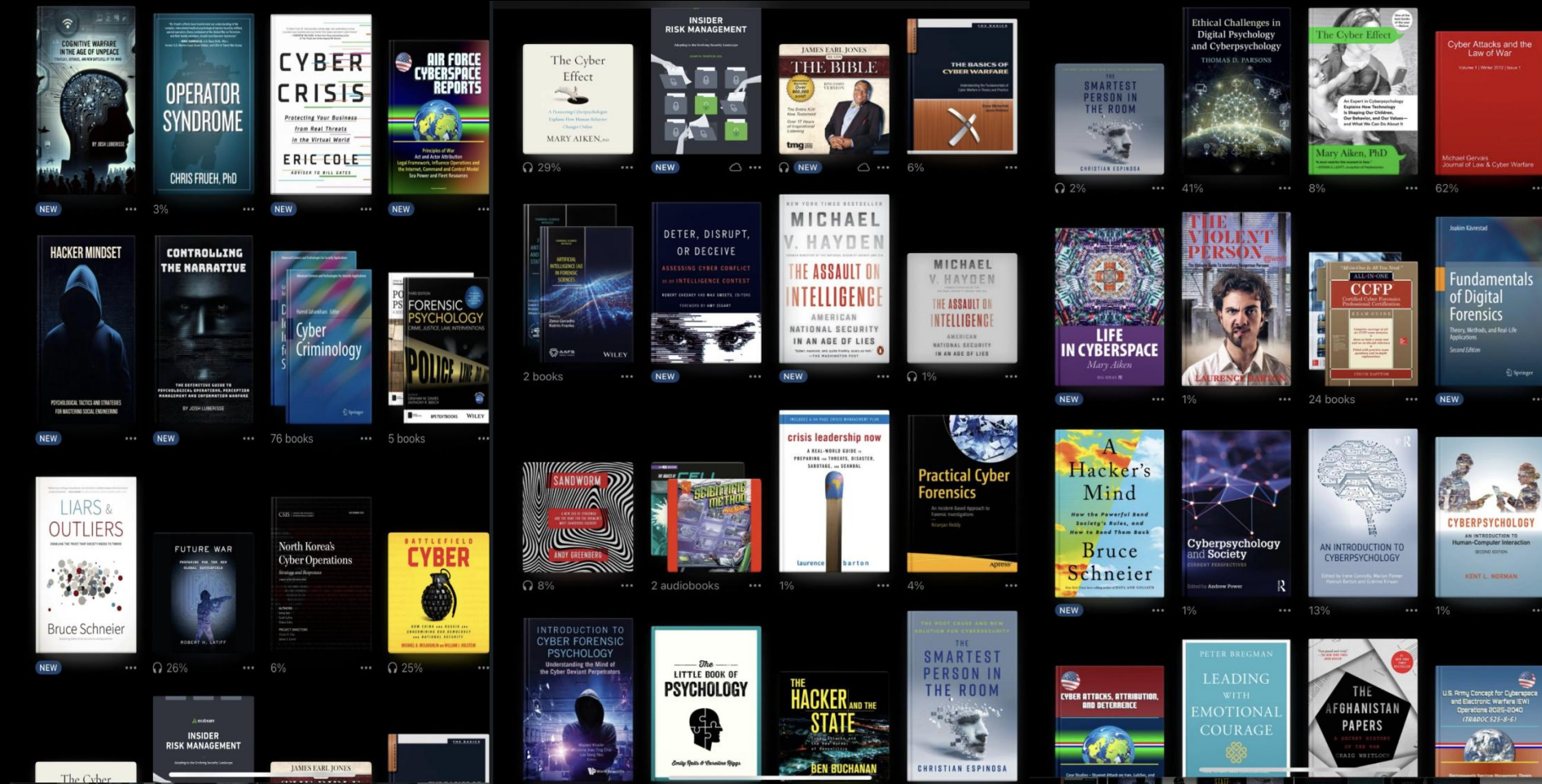
£10.8 You could take an extra £10,884 this year* Find out more

CULTURE

CSI Reboots Its Franchise With Cybercrime Show

BY LAUREN WALKER / FEBRUARY 24, 2015 1:28 PM EST

CYBERPSYCHOLOGY RESOURCES



THANK YOU

- Aiken, M. P. (2016). The Cyber Effect. New York. Random House, Spiegel & Grau.
- Connolly, et al.(2016). Introduction to Cyberpsychology. An Introduction to Cyberpsychology (pp. 3-14). New York, NY: Routledge.
- Joinson et al., (2009) Oxford Handbook of Internet Psychology
- Norman, K. (2008) Cyberpsychology: An Introduction to Human-Computer Interaction Cambridge: Cambridge University Press
- Martineau, M.; Spiridon, E.; Aiken, M. A Comprehensive Framework for Cyber Behavioral Analysis Based on a Systematic Review of Cyber Profiling Literature. Forensic Sci. 2023, 3, 452-477.
- Suler, J. (2004). The online disinhibition effect. Cyberpsychology & Behavior, 7(3), 321
- Rich, M.S.; Aiken, M.P. An Interdisciplinary Approach to Enhancing Cyber Threat Prediction Utilizing Forensic Cyberpsychology and Digital Forensics. Forensic Sci. 2024, 4, 110-151.
- Lundie, M., Aiken, M.P., Amos-Binks, A., Lindke, K. & Janosek, J. (2024) The Enterprise Strikes Back: Conceptualizing the HackBot - Reversing Social Engineering in the Cyber Defense Context. Proceedings of the 57th Hawaii International Conference on System Sciences (HICSS)
- Martineau, M.; Spiridon, E.; Aiken, M. A Comprehensive Framework for Cyber Behavioral Analysis Based on a Systematic Review of Cyber Profiling Literature. Forensic Sci. 2023, 3, 452-477.
- Martineau, M., Spiridon, E., & Aiken, M. (2024). Pathways to Criminal Hacking: Connecting Lived Experiences with Theoretical Explanations. Forensic Sciences, 4(4), 647-668.
- Coleman, K, Aiken, M. P & Keegan, D, et al., (2021) "A New Smartphone Optic Nerve Head Biometric for Verification and Change Detection" Journal of Translational Vision Science & Technology (TVST).
- Joint Chiefs of Staff, Joint Publication 3-12 Cyberspace Operations (2018)



HYBRID
IDENTITY
PROTECTION
conf25

