



Verizon  
SUB

Verizon  
SUB

Best in America.  
Best in New York.



verizon

OUTLET



verizon





VIE

Email or Phone

eamoroso@att.net

Password

.....

Log In

Forgot account?



Verizon

@verizon

[Home](#)[Posts](#)[Locations](#)[Videos](#)[Photos](#)[About](#)[Community](#)[Create a Page](#)[Like](#)[Share](#)[Suggest Edits](#)

...

[Send Message](#)

## Posts



Verizon

1 hr ·

Getting to our cell sites to make sure they never stop working is one of the reasons why we are America's most awarded network.

## Verizon

Company

## Community

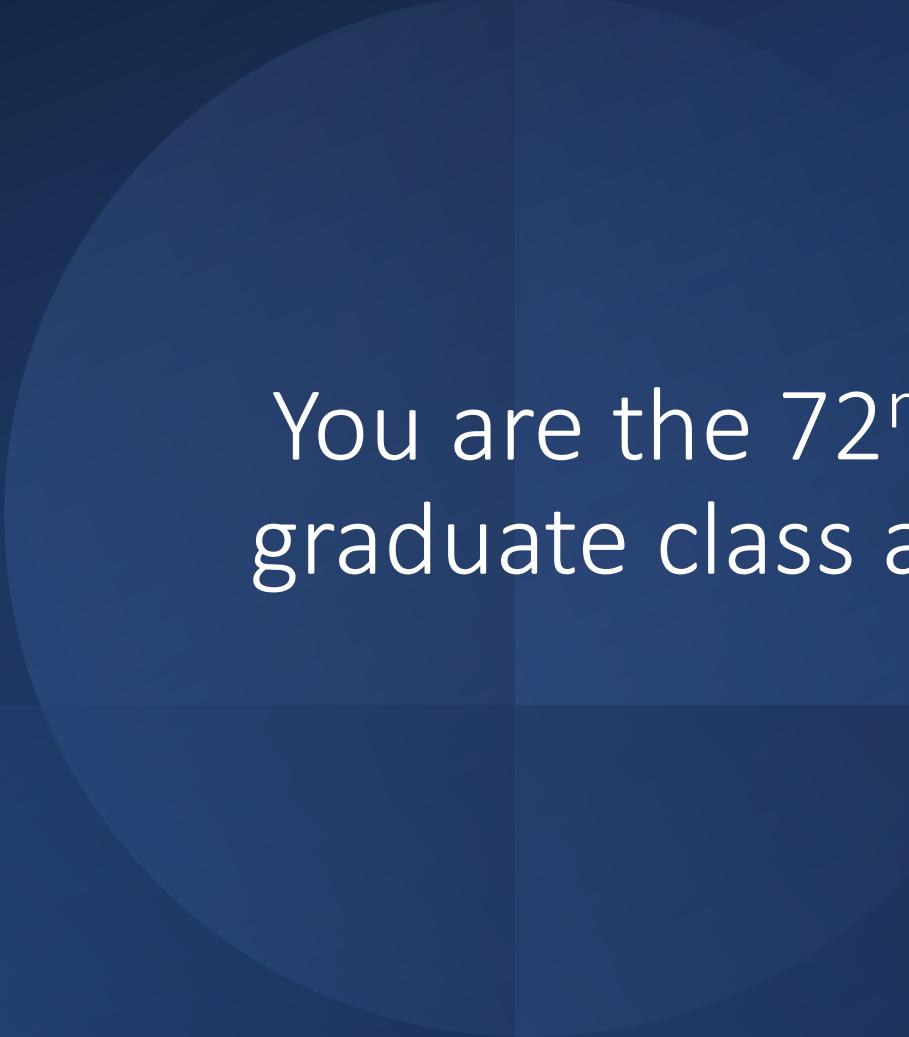
[See All](#)

7,383,659 people like this

[See more of Verizon on Facebook](#)[About](#)[See All](#)

Welcome to the longest running graduate  
cybersecurity course in the world.

eamoroso@tag-cyber.com



You are the 72<sup>nd</sup> consecutive CS 573  
graduate class at Stevens since 1990.

How much has technology  
changed since 1990?

1990

You'd expect to see phones this advanced aboard intergalactic star cruisers and on far-off planets. Now they exist here on earth, and are brought to you by Panasonic.

#### Video Phone

It seems like every sci-fi movie ever made has had a video phone in it. Today there's a video phone from Panasonic. While you talk, it actually receives or transmits a black-and-white still picture every 6.5 seconds. The Panasonic video phone uses existing phone lines and

### Once phones like these were science fiction. Now they're from Panasonic.

phone jacks. So your video phone call won't cost any more than a regular phone call.

#### FAX+ System

Whenever star command sent secret plans, they came over a device very similar to the Panasonic FAX+ System. The FAX+ System can receive and transmit letters, charts, even photographs in a flash. It's also a sophisticated phone system with a built-in answering machine. And because this advanced system can do everything over a single phone line, you won't need a costly second line.

#### Integrated Telephone

This Panasonic integrated telephone answering system seems to have an intelligence all its own. Its Auto-Logic™ function plays back messages and resets the answering machine with the touch of one button. It can also be programmed to transfer your messages to any other phone. This Panasonic phone can even memorize up to 26 numbers and dial them for you.

#### Folding Cordless Phone

If we didn't tell you that this folding cordless phone was from Panasonic, you'd think it was directly from a sci-fi movie. So compact, this Panasonic cordless phone can fold up and be concealed in a pocket. It even has a built-in intercom for direct wireless communication between you and the base.

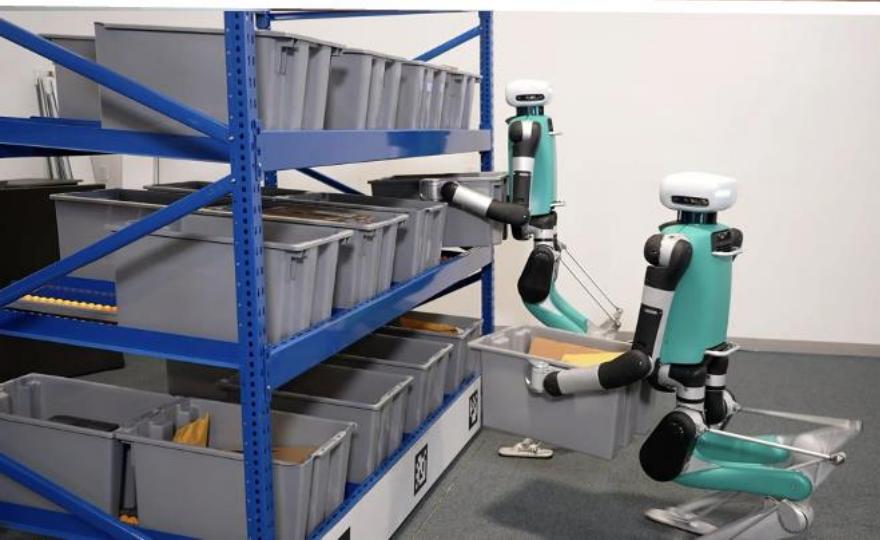
Once phones this advanced were science fiction. Today they're science fact. And they're from Panasonic.

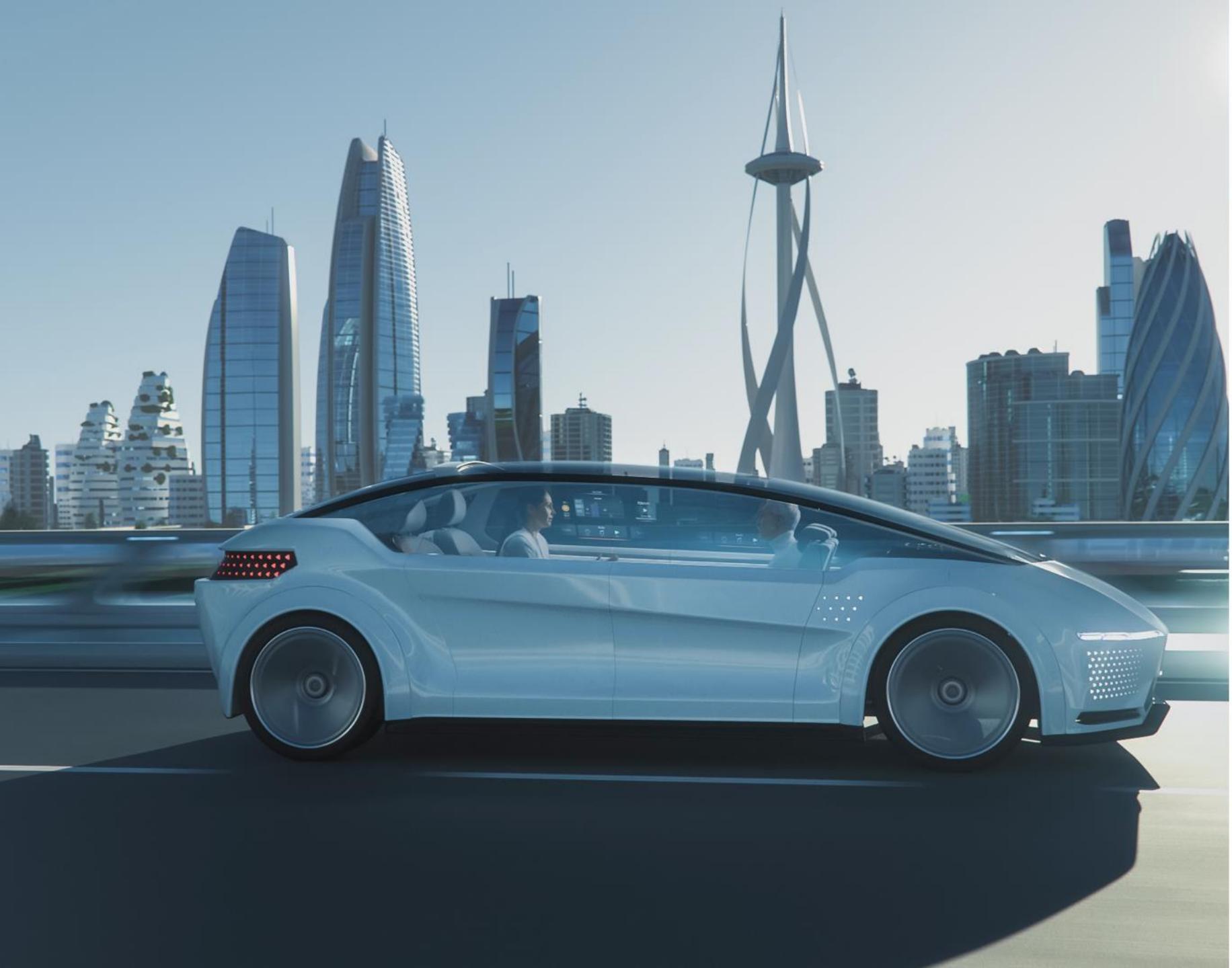
**Panasonic**  
just slightly ahead of our time

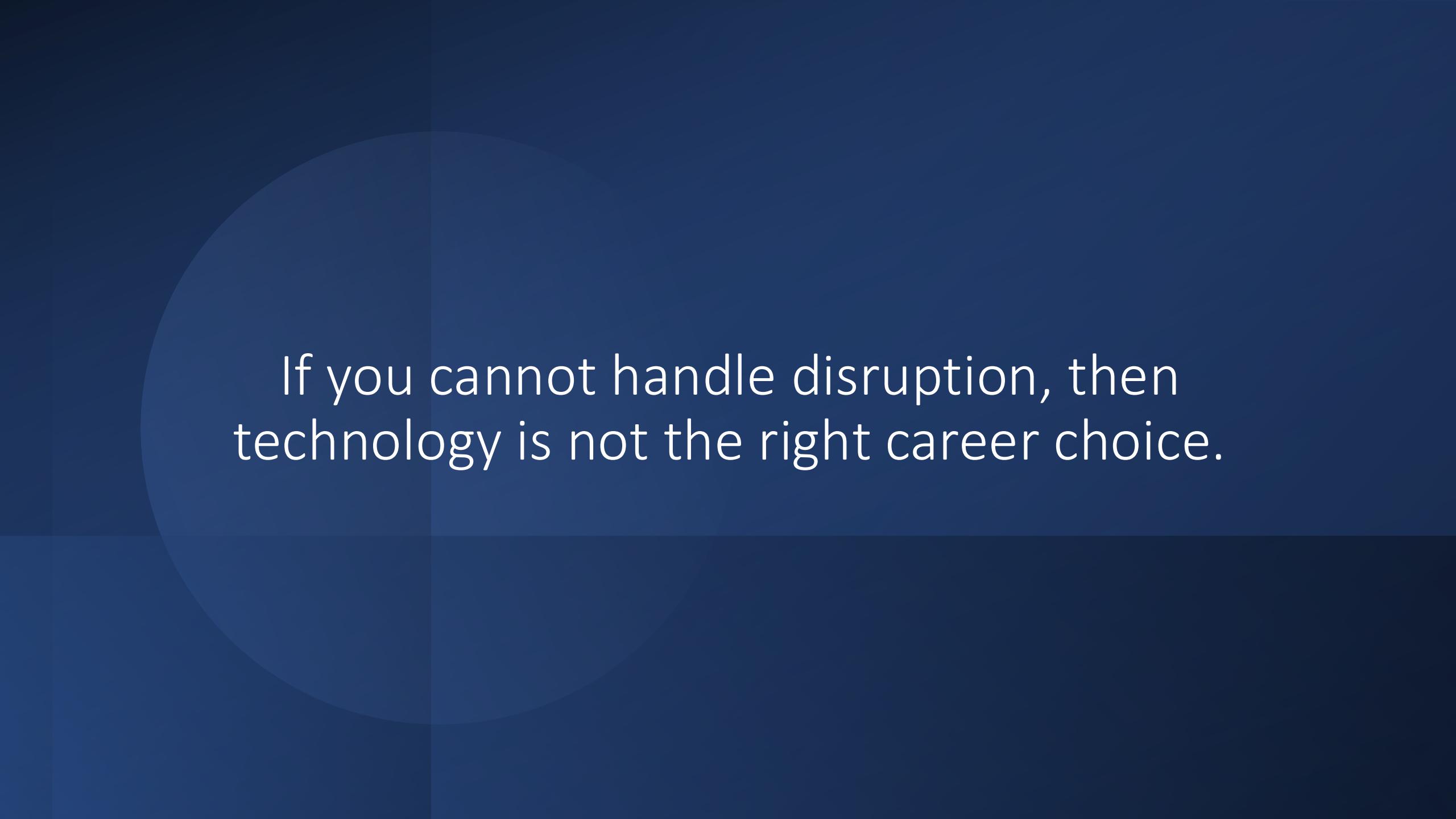


Video Phone operates with existing telephone. Video Phone picture simulated.  
These telephones are tone/pulse switchable and are capable of accessing tone-activated computer systems.

2025





The background features a dark blue gradient with three semi-transparent white circles of varying sizes. One circle is positioned in the upper left, another in the lower center, and a third in the lower right.

If you cannot handle disruption, then  
technology is not the right career choice.



Most cybersecurity guidance is  
terrible.

## BLOG

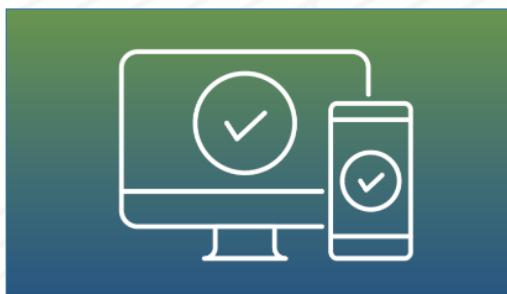
# 4 Things You Can Do To Keep Yourself Cyber Safe

**Released:** December 18, 2022

**RELATED TOPICS:** [CYBERSECURITY BEST PRACTICES](#)



## 4 Things to Keep You Cyber Safe



### Turn on Multifactor Authentication

Implement [multifactor authentication](#) on your accounts and make it



### Update Your Software

Update your software. In fact, turn on automatic updates.



### Think Before You Click

Think before you click. More than 90% of successful cyber-attacks start with a phishing email.



### Use Strong Passwords

Use strong passwords, and ideally a password manager to generate and store unique passwords.

## BLOG

# 4 Things You Can Do To Keep Yourself Cyber Safe

Released: December 18, 2022

RELATED TOPICS: [CYBERSECURITY BEST PRACTICES](#)

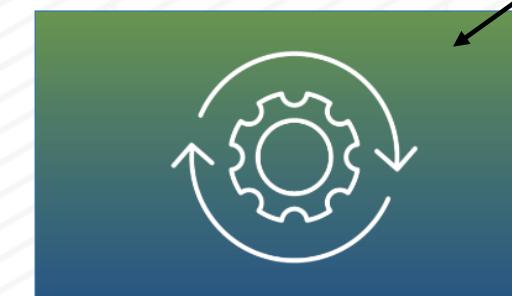
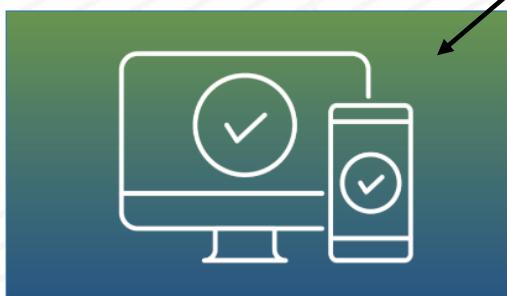


## 4 Things to Keep You Cyber Safe

*Easily Social Engineered*

*Irrelevant To Most Attacks*

*Won't Help Stop Most Attacks*



### Turn on Multifactor Authentication

Implement [multifactor authentication](#) on your accounts and make it

### Update Your Software

Update your software. In fact, turn on automatic updates.

### Think Before You Click

Think before you click. More than 90% of successful cyber-attacks start with a phishing email.

### Use Strong Passwords

Use strong passwords, and ideally a password manager to generate and store unique passwords.

[← Back to Blog](#)

CYBERSECURITY

# How To Get Into Cybersecurity With No Experience 🤖 [Job Guide]

15 minute read | March 28, 2024



Written by:  
Monica J. White

## Magic Quadrant

Figure 1. Magic Quadrant for Cloud Access Security Brokers



## Magic Quadrant

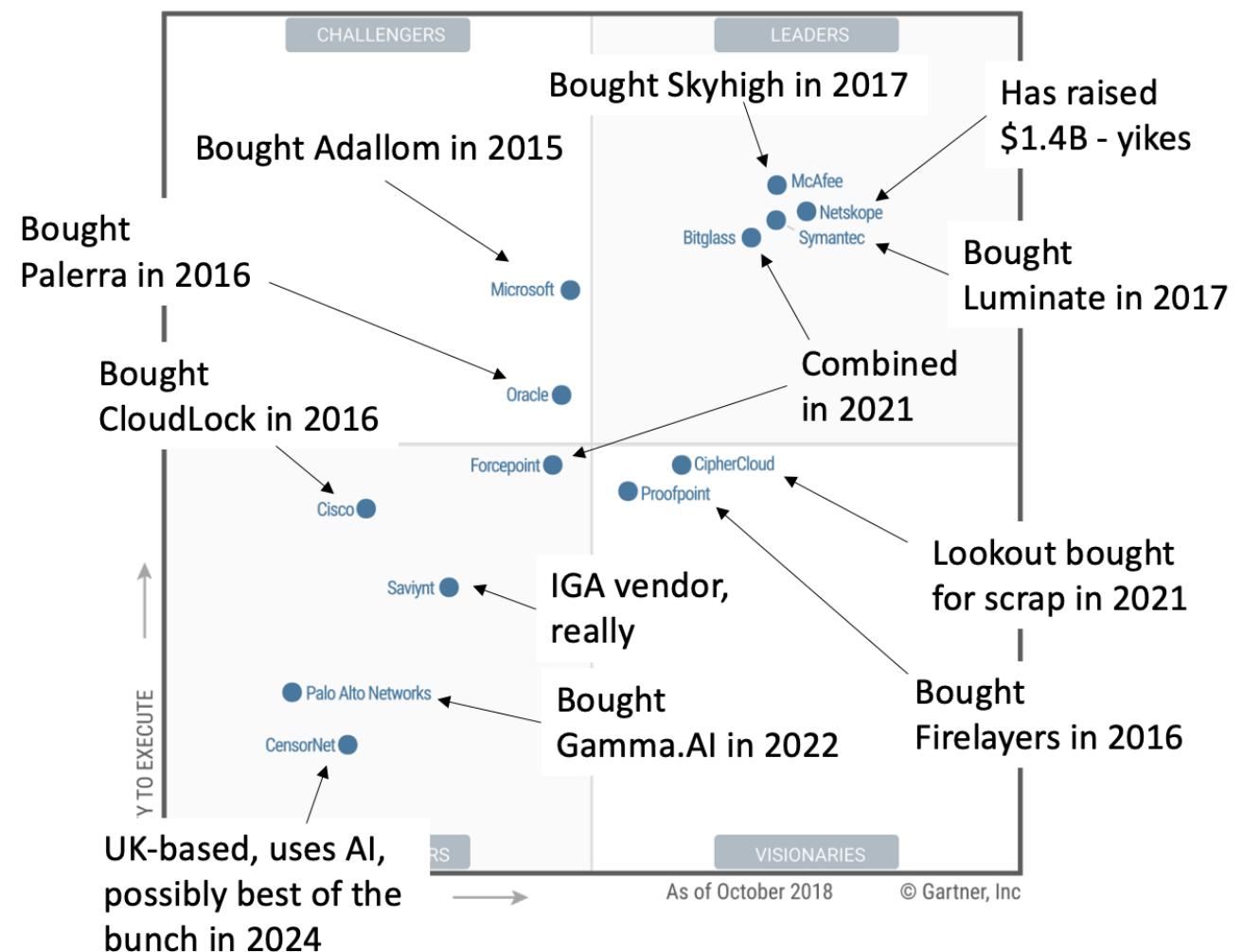
Figure 1. Magic Quadrant for Cloud Access Security Brokers



Source: Gartner (October 2018)

## Magic Quadrant

Figure 1. Magic Quadrant for Cloud Access Security Brokers





The most important thing you can learn about cybersecurity is best illustrated with a barn.



Where would you enter  
this barn, if you wanted  
to steal something  
inside?



Would you agree that  
99% of thieves would  
enter through the  
open door?



Does closing the barn door make the barn safe from future theft?



Does closing the barn  
side door make the barn  
safe from future  
theft?





tomorrow  
belongs to those who embrace it  
today

[trending](#)[tech](#)[innovation](#)[business](#)[security](#)[advice](#)[buying guides](#)

/ tech

[Home](#) / [Tech](#) / [Security](#)

# Cybersecurity: 99% of email attacks rely on victims clicking links

**Social engineering is by far the biggest factor in malicious hacking campaigns, warn researchers – so how can it be stopped?**

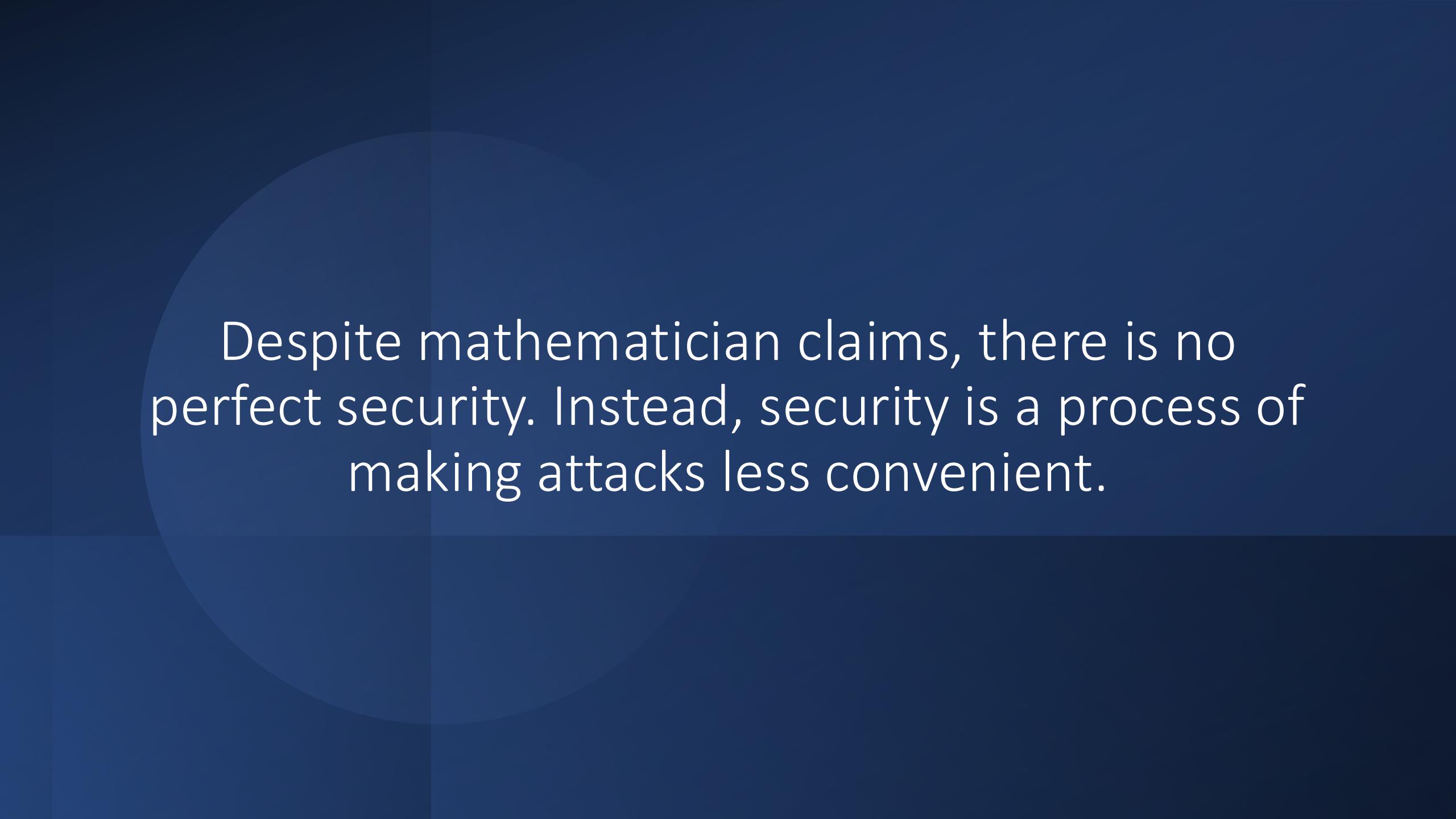


Written by **Danny Palmer**, Senior Writer

Sept. 9, 2019 at 9:10 a.m. PT



## What Should You Conclude From This Measurement?

The background features a dark blue gradient with three semi-transparent white circles of varying sizes. One circle is centered at the top, another is positioned in the middle left, and a third is located at the bottom left.

Despite mathematician claims, there is no perfect security. Instead, security is a process of making attacks less convenient.

This class is intended as a safe zone  
for exploring new ideas and discussing  
concepts in cyber.

# How Does Innovation Affect Security?



**1890 – 1930: Forty Years of Invention in Science and Technology**

Gamow  
THIRTY YEARS THAT SHOOK PHYSICS

History of Quantum Physics

Gamow

# THIRTY YEARS THAT SHOOK PHYSICS

D



**Vannevar Bush – MIT Computer in 1930, Founder of Raytheon**

Albert Einstein  
Old Grove Rd.  
Nassau Point  
Peconic, Long Island  
August 2nd, 1939

F.D. Roosevelt,  
President of the United States,  
White House  
Washington, D.C.

Sir:

Some recent work by E. Fermi and L. Szilard, which has been communicated to me in manuscript, leads me to expect that the element uranium may be turned into a new and important source of energy in the immediate future. Certain aspects of the situation which has arisen seem to call for watchfulness and, if necessary, quick action on the part of the Administration. I believe therefore that it is my duty to bring to your attention the following facts and recommendations:

In the course of the last four months it has been made probable - through the work of Joliot in France as well as Fermi and Szilard in America - that it may become possible to set up a nuclear chain reaction in a large mass of uranium, by which vast amounts of power and large quantities of new radium-like elements would be generated. How it appears almost certain that this could be achieved in the immediate future.

This new phenomenon would also lead to the construction of bombs, and it is conceivable - though much less certain - that extremely powerful bombs of a new type may thus be constructed. A single bomb of this type, carried by boat and exploded in a port, might very well destroy the whole port together with some of the surrounding territory. However, such bombs might very well prove to be too heavy for transportation by air.

-2-

The United States has only very poor ores of uranium in moderate quantities. There is some good ore in Canada and the former Czechoslovakia, while the most important source of uranium is Belgian Congo.

In view of this situation you may think it desirable to have some permanent contact maintained between the Administration and the group of physicists working on chain reactions in America. One possible way of achieving this might be for you to entrust with this task a person who has your confidence and who could perhaps serve in an unofficial capacity. His task might comprise the following:

a) to approach Government Departments, keep them informed of the further development, and put forward recommendations for Government action, giving particular attention to the problem of securing a supply of uranium ore for the United States;

b) to speed up the experimental work, which is at present being carried on within the limits of the budgets of University laboratories, by providing funds, if such funds be required, through his contacts with private persons who are willing to make contributions for this cause, and perhaps also by obtaining the co-operation of industrial laboratories which have the necessary equipment.

I understand that Germany has actually stopped the sale of uranium from the Czechoslovakian mines which she has taken over. That she should have taken such early action might perhaps be understood on the ground that the son of the German Under-Secretary of State, von Weizsäcker, is attached to the Kaiser-Wilhelm-Institut in Berlin where some of the American work on uranium is now being repeated.

Yours very truly,  
*A. Einstein*  
(Albert Einstein)

1939: Einstein Letter to FDR



**1968 - 2008: Forty Years of Innovation in Computing and Software**



**Has Modern Computing Been More Influential Than Gutenberg?**

A photograph of the main entrance to Boston Children's Hospital. The building is a light-colored stone structure with large glass doors. A blue sign above the entrance reads "Children's Hospital" in white letters. Below that, another blue sign says "Ranked #1 – U.S. News & World Report" with the U.S. News logo on either side. Underneath those signs, the words "Main Entrance" are written in white. In front of the building, there are several people walking on the sidewalk, some cars parked along the street, and traffic lights. The sky is overcast.

**Children's Hospital**

Ranked #1 – U.S. News & World Report

Main Entrance

DOJ charges 3 Iranian citizens in  
attempted cyber-attack on Boston Children's



**The Terrible Downside of Four Decades of Computing Innovation.**

This is why we study cybersecurity.

What Can Be Learned from the  
Early (Mischievous) Hacks?

Yippie!

Glib

June, 1971.  
Through the  
generous  
contribution of  
**steal  
this  
book**

BY ABBIE HOFFMAN

Co-conspirator: Izack Haber

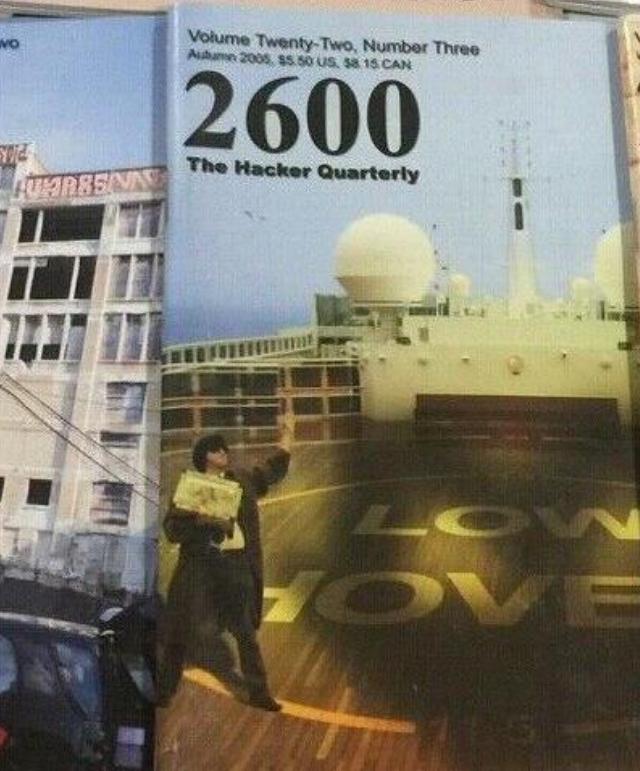
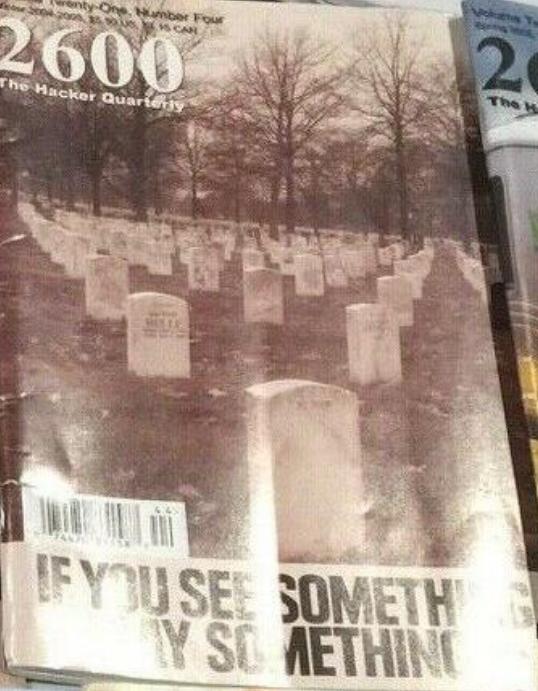
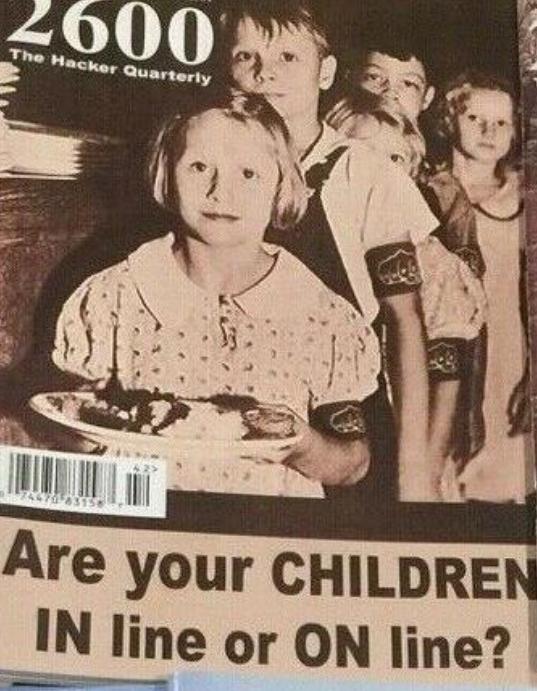
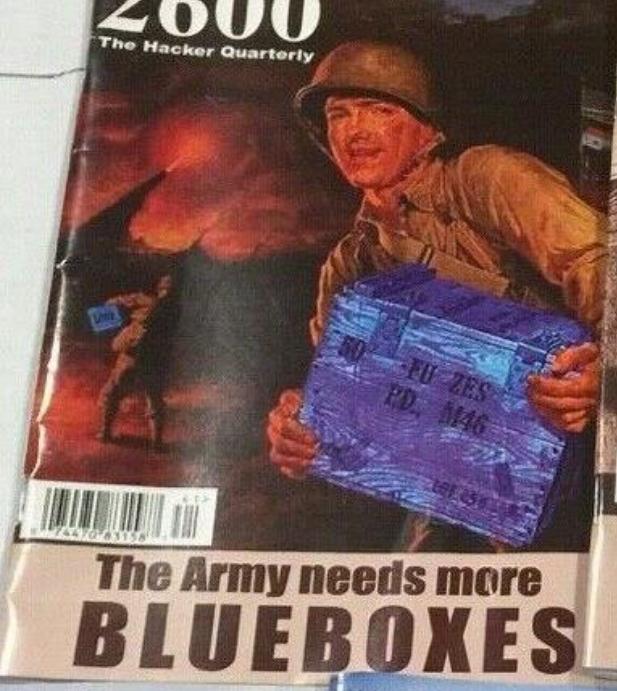
Accessories after the Fact: Tom Forcade  
Bert Cohen

Distributed by  
Grove Press, Inc. New York



PIRATE EDITIONS •





KIE

430 4E 1

78 07/29/08

NOT DELIVERABLE AS ADDRESSED  
RETURN TO SENDER  
UNABLE TO FORWARD

19027028282

\*0746-00719-29-25

||||||||||||||||||||||||||||||

# Understanding the Hack: 70's Vintage Soda Machine



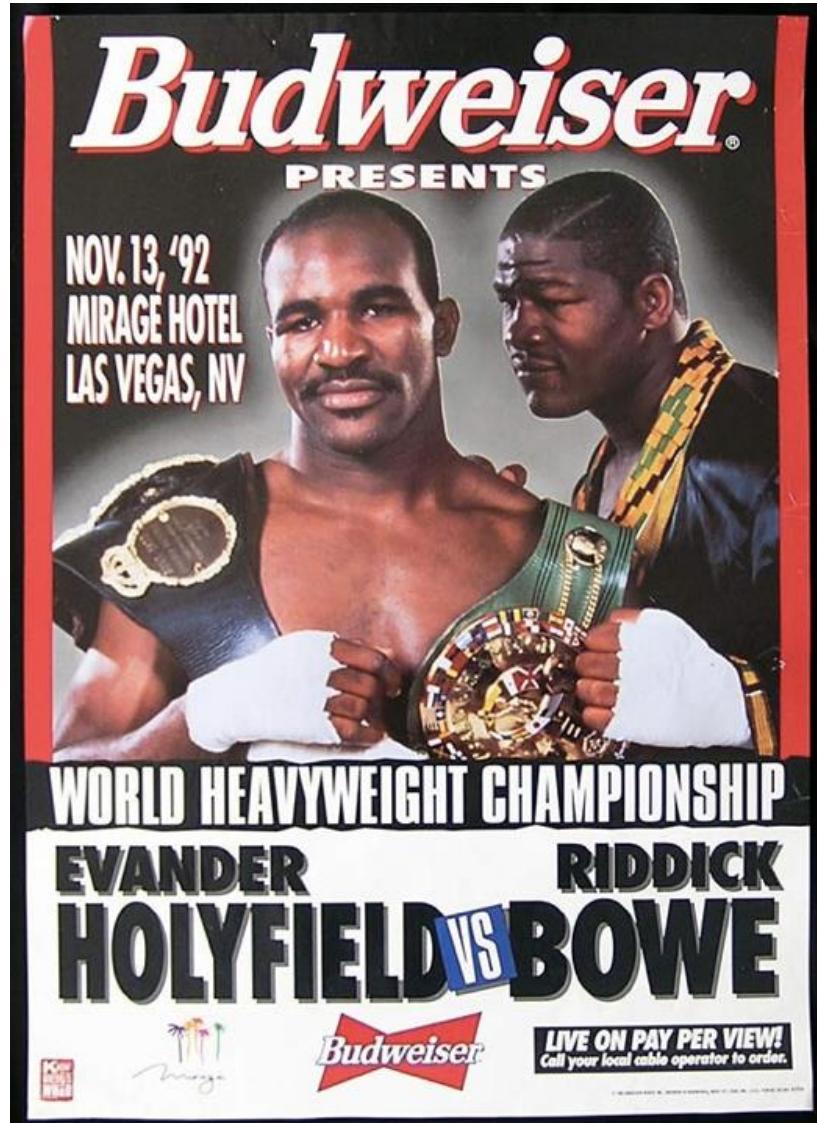
# Understanding the Hack: Early Scams and Social Engineering



Victor Lustig

# Understanding the Hack: Unauthorized Infrastructure Access



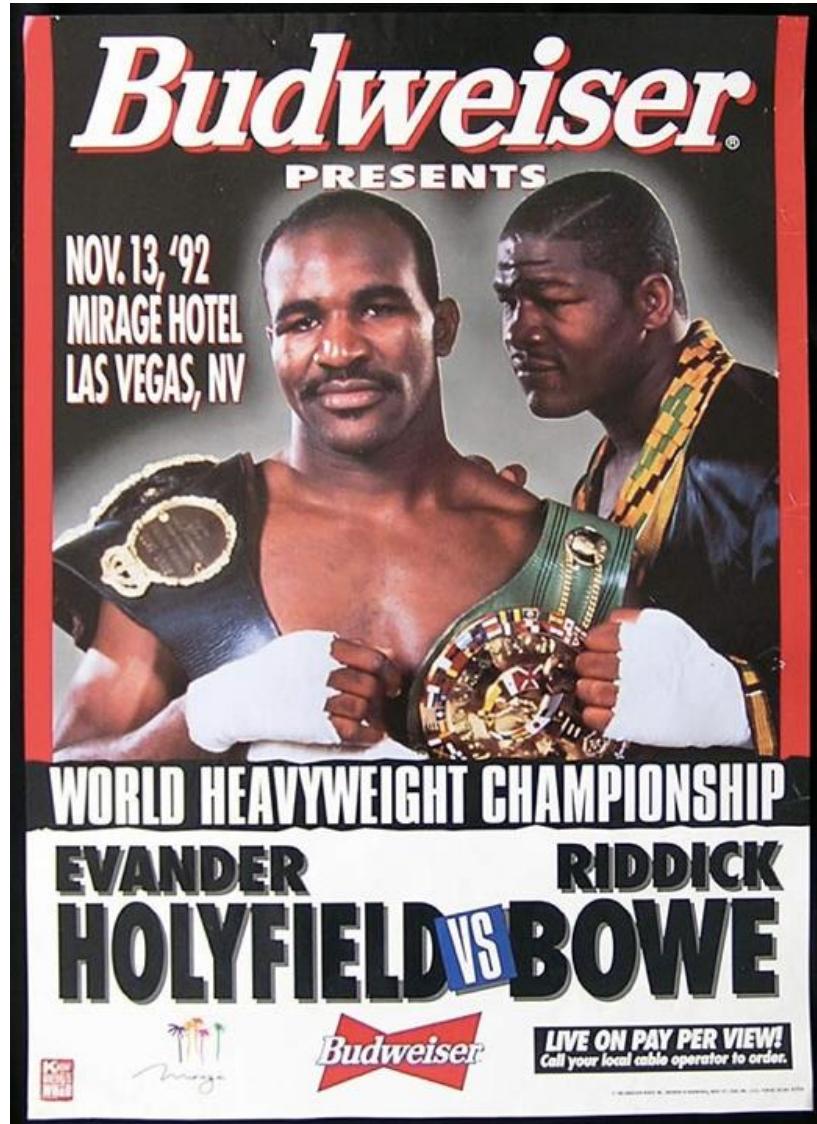


Scrambled Picture for Non-Payers



Trinitron



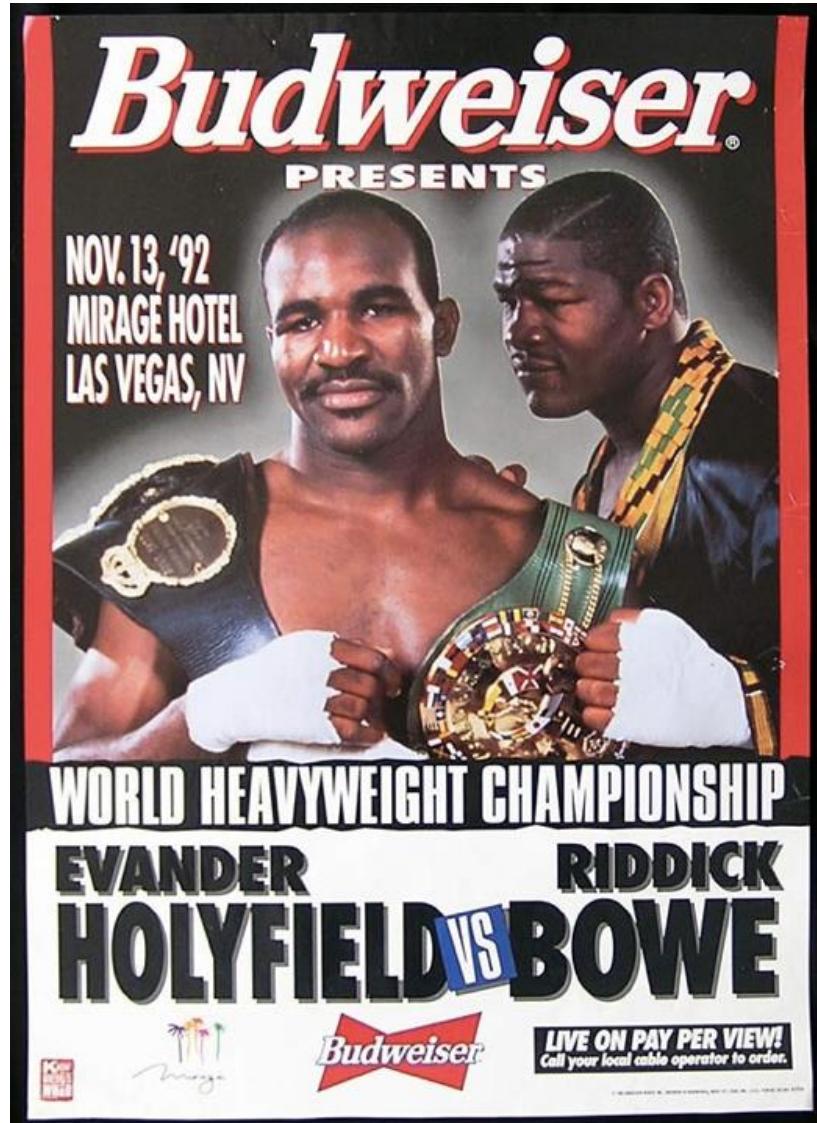


Continental Cablevision of Hartford broadcast a special offer of a free T-shirt during last fall's Holyfield/Bowe fight (14 Nov 92). Unlike most pay-per-view broadcasting, this one did not show up through legitimate decoders.

The ad and its 800 number only showed up when watched through illegal decoders. 140 freeloaders called the 800 number within minutes of the ad's broadcast.

Continental sent the T-shirts by certified, return receipt mail, and then sent them a follow-up letter reminding them of the federal law (fines up to \$10,000) and demanding a \$2000 fine.

[Chicago Tribune, 3 Feb 1993]



Fake Enticement for Fraudsters

Technologists tend to ignore history. We will not make that mistake here.



# Can Government Manage Critical Infrastructure Cyber Risk?





## PDD-63



"As part of a national warning and information sharing system, the President authorizes ... a full scale *National Infrastructure Protection Center* (NIPC)..."

"This organization shall serve as a national critical infrastructure *threat assessment, warning, vulnerability, and law enforcement and response entity*..."

# Protecting Critical Assets (National Infrastructure) – 1998



BRIEFING ROOM

## Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The

# Protecting Critical Assets (National Infrastructure) – 2021



## Biden's Executive Order Will Not Stop Cyber Attacks

Edward Amoroso on LinkedIn • 3 min read

On May 12, 2021, President Joseph Biden signed the "Executive Order on Improving the...

# Recent Concern Regarding National Infrastructure Protection



## Predicting the Impact of Trump's Election on Cyber

Edward Amoroso

Below are seven predictions from our team at TAG for how the recent Trump election of 202...



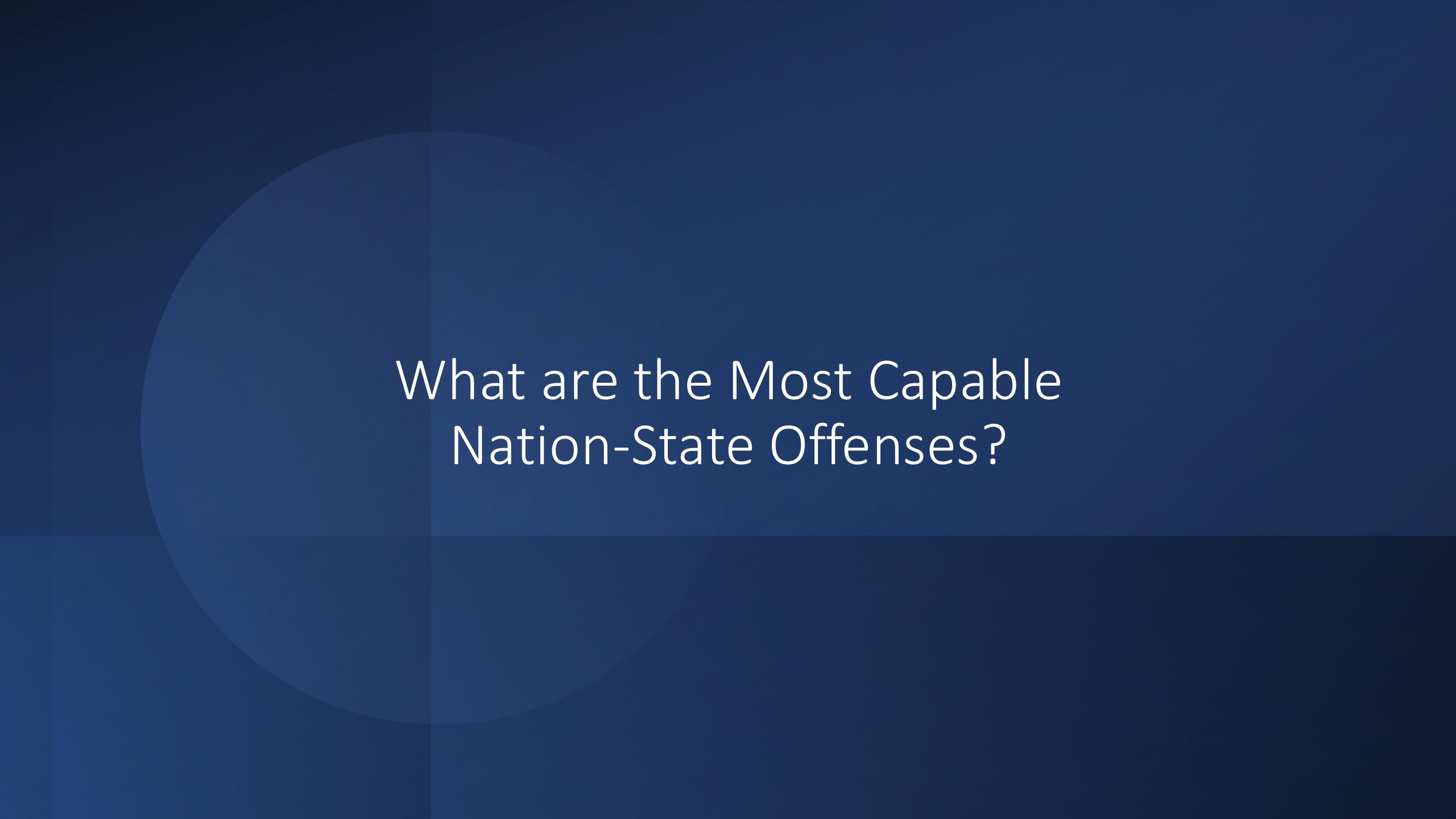
You and 316 others

83 comments · 24 reposts

Please Follow me on LinkedIn (Just Follow – Cannot Connect)



CISOs in public companies are being targeted  
by the SEC. (I do not approve.)

The background features a dark blue gradient with three semi-transparent white circles of varying sizes. One circle is positioned in the upper left, another in the lower center, and a third in the lower right.

# What are the Most Capable Nation-State Offenses?

**Name Five Countries That Claim 100% Success Rates in Every Offensive Campaign, Regardless of the Target Defense:**

- 1.
- 2.
- 3.
- 4.
- 5.

# Name Five Countries That Claim 100% Success Rates in Every Offensive Campaign, Regardless of the Target Defense:

1. US
- 2.
- 3.
- 4.
- 5.



# Name Five Countries That Claim 100% Success Rates in Every Offensive Campaign, Regardless of the Target Defense:

1. US
2. China
- 3.
- 4.
- 5.



# Name Five Countries That Claim 100% Success Rates in Every Offensive Campaign, Regardless of the Target Defense:

1. US
2. China
3. Russia
- 4.
- 5.



**Name Five Countries That Claim 100% Success Rates in Every Offensive Campaign, Regardless of the Target Defense:**

- 1. US**
- 2. China**
- 3. Russia**
- 4. Israel**
- 5.**

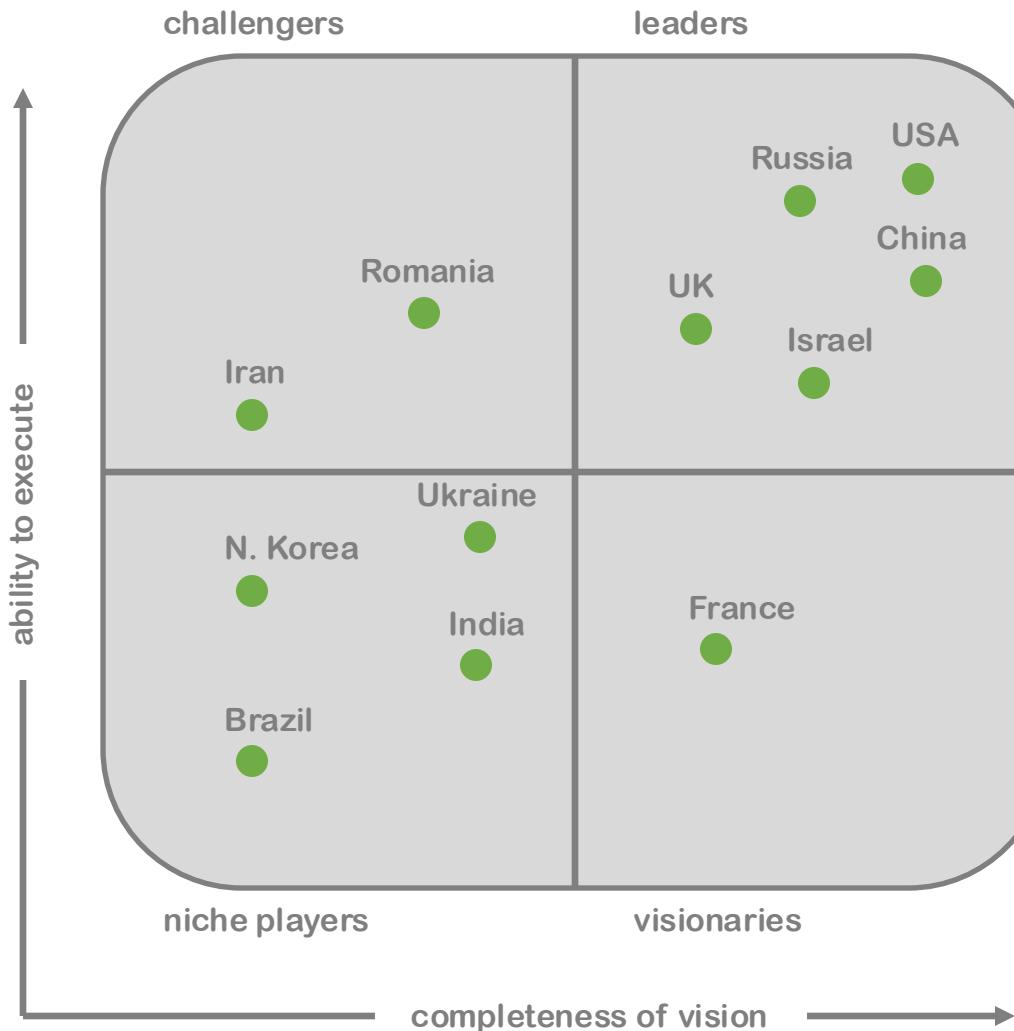


**Name Five Countries That Claim 100% Success Rates in Every Offensive Campaign, Regardless of the Target Defense:**

- 1. US**
- 2. China**
- 3. Russia**
- 4. Israel**
- 5. UK**



# Advanced Persistent Threat (APT) Global Actors



1. USA, Russia, China, Israel, and the UK have ~ 100% success rates on offensive APT cyber operations
2. North Korea derives ~100% of its APT cyber operations capability via training and support from China
3. Romania, Iran, and Ukraine have large populations of technically trained, under-employed youth

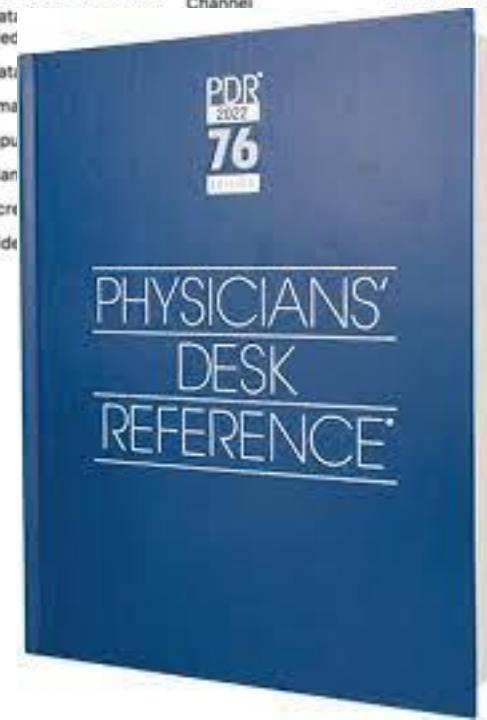
# How Do We Model Attack Strategy?

# MITRE ATT&CK Framework

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	31 items	56 items	28 items	59 items	20 items	19 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	Appinit DLLs	Appinit DLLs	Bypass User Account Control	Credential Dumping	Credentials in Files	Data from Information Repositories	Data Transfer Size Limits	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Registry	File and Directory Discovery	Exploitation of Remote Services	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Attachment	Execution through API	Authentication Package	Authentication Package	CMSTP	Credentials in Registry	Exploitation for Credential Access	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Exfiltration Over Command and Control Channel
Spearphishing Link	Execution through Module Load	BITS Jobs	Bypass User Account Control	Code Signing	Forced Authentication	Network Share Discovery	Pass the Hash	Pass the Ticket	Data from Removable Media	Data Encoding
Spearphishing via Service	Exploitation for Client Execution	Bootkit	DLL Search Order Hijacking	Component Firmware	Hijacking	Component Object Model Hijacking	Hooking	Remote Desktop Protocol	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Graphical User Interface	Browser Extensions	Change Default File Association	Dylib Hijacking	Control Panel Items	Control Panel Items	Input Capture	Password Policy Discovery	Data Staged	Domain Fronting
Supply Chain Compromise	InstallUtil	Component Firmware	Component Object Model Privilege Escalation	Dylib Hijacking	DCShadow	DCShadow	Input Prompt	Peripheral Device Discovery	Remote File Copy	Fallback Channels
Trusted Relationship	Launchctl	Component Object Model	Extra Window Memory Injection	Deobfuscate/Decode Files or Information	Deobfuscate/Decode Files or Information	Deobfuscate/Decode Files or Information	Kerberoasting	Remote Services	Email Collection	Multi-hop Proxy
Valid Accounts	Local Job Scheduling	Hijacking	Hijacking	Disabling Security Tools	Keychain	Keychain	Input Capture	Input Capture	Input Capture	Multi-Stage Channels
	LSASS Driver	Create Account	File System Permissions Weakness	LLMNR/NBT-NS Poisoning	LLMNR/NBT-NS Poisoning	LLMNR/NBT-NS Poisoning	Man in the Browser	Man in the Browser	Man in the Browser	Multiband Communication
	Mshta	DLL Search Order Hijacking	Hijacking	DLL Search Order Hijacking	Network Sniffing	Network Sniffing	Peripheral Device Discovery	Peripheral Device Discovery	Screen Capture	Multilayer Encryption
	PowerShell	Dylib Hijacking	Image File Execution Options Injection	Exploitation for Defense Evasion	>Password Filter DLL	>Password Filter DLL	Pass the Hash	Pass the Hash	Video Capture	Port Knocking
	Regsvcs/Regasm	External Remote Services	Options Injection	Process Discovery	Process Discovery	Process Discovery	Remote System Discovery	Remote System Discovery	Taint Shared Content	Remote Access Tools
	Regsvr32	File System Permissions Weakness	Launch Daemon	Query Registry	Query Registry	Query Registry	Third-party Software	Third-party Software	Third-party Software	Remote File Copy
	Rundll32	New Service	Extra Window Memory Injection	Replication Through Removable Media	Replication Through Removable Media	Replication Through Removable Media	Windows Admin Shares	Windows Admin Shares	Windows Admin Shares	Standard Application Layer Protocol
	Scheduled Task	Path Interception	File System Logical Offsets	Security Software Discovery	Security Software Discovery	Security Software Discovery	Windows Remote Management	Windows Remote Management	Windows Remote Management	Standard Cryptographic Protocol
	Scripting	Plist Modification	Gatekeeper Bypass	System Information Discovery	System Information Discovery	System Information Discovery				Standard Non-Application Layer Protocol
	Service Execution	Hidden Files and Directories	Hidden Files and Directories	Two-Factor Authentication Interception	Two-Factor Authentication Interception	Two-Factor Authentication Interception				Uncommonly Used Port
	Signed Binary Proxy Execution	HyperV	Hidden Users	System Network Configuration Discovery	System Network Configuration Discovery	System Network Configuration Discovery				Web Service
	Signed Script Proxy Execution	Image File Execution Options Injection	Scheduled Task	System Network Connections Discovery	System Network Connections Discovery	System Network Connections Discovery				
	Source	Kernel Modules and Extensions	Service Registry Permissions Weakness	HISTCONTROL	HISTCONTROL	HISTCONTROL	System Owner/User Discovery	System Owner/User Discovery	System Owner/User Discovery	
	Space after Filename	Setuid and Setgid	Image File Execution Options Injection	System Service Discovery	System Service Discovery	System Service Discovery				

# MITRE ATT&CK Framework

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	31 items	56 items	28 items	59 items	20 items	19 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	Appinit DLLs	Appinit DLLs	Bypass User Account Control	Credential Dumping	Credentials in Files	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Registry	File and Directory Discovery	Data from Local System	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Attachment	Execution through API	Authentication Package	Authentication Package	CMSTP	Code Signing	Exploitation for Credential Access	Logon Scripts	Logon Scripts	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing Link	Execution through Module Load	BITS Jobs	Bypass User Account Control	DLL Search Order Hijacking	Component Firmware	Forced Authentication	Network Share Discovery	Pass the Hash	Pass the Ticket	
Spearphishing via Service	Exploitation for Client Execution	Bootkit	Component Object Model Hijacking	Component Object Model Hijacking	Hooking	Input Capture	Network Share Discovery	Pass the Ticket	Pass the Ticket	
Supply Chain Compromise	Graphical User Interface	Browser Extensions	Change Default File Association	Dylib Hijacking	Control Panel Items	Periphera	>Password Policy Discovery	Remote Desktop Protocol	Remote Desktop Protocol	
Supply Chain Compromise	InstallUtil	Component Firmware	Component Object Model Hijacking	Exploitation for Privilege Escalation	DCShadow	Input Prompt	Peripheral Device Discovery	Remote File Copy	Remote File Copy	
Trusted Relationship	Launchctl	Component Object Model Hijacking	Extra Window Memory Injection	Deobfuscate/Decode Files or Information	Deobfuscate/Decode Files or Information	Kerberoasting	Remote Services	Remote Services	Remote Services	
Valid Accounts	Local Job Scheduling	Create Account	File System Permissions Weakness	Disabling Security Tools	Keychain	Permission Groups Discovery	Replication Through Removable Media	Replication Through Removable Media	Replication Through Removable Media	
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	DLL Side-Loading	LLMNR/NBT-NS Poisoning	Process Discovery	Shared Webroot	Shared Webroot	Shared Webroot	
	Mshta	Dylib Hijacking	Image File Execution Options Injection	Network Sniffing	Query Registry	SSH Hijacking	Taint Shared Content	Taint Shared Content	Taint Shared Content	
	PowerShell	External Remote Services	Path Interception	Exploitation for Defense Evasion	Private Keys	Third-party Software	Third-party Software	Third-party Software	Third-party Software	
	Regsvcs/Regasm	File System Permissions Weakness	Launch Daemon	Extra Window Memory Injection	Replication Through Removable Media	Windows Admin Shares	Windows Admin Shares	Windows Admin Shares	Windows Admin Shares	
	Regsvr32	New Service	File Deletion	Security Software Discovery	Security Software Discovery	Windows Remote Management	Windows Remote Management	Windows Remote Management	Windows Remote Management	
	Rundll32	Path Interception	File System Logical Offsets	Securityd Memory	System Information Discovery					
	Scheduled Task	Plist Modification	Gatekeeper Bypass	Two-Factor Authentication Interception	System Network Configuration Discovery					
	Scripting	Port Monitors	Hidden Files and Directories	Hidden Users	System Network Connections Discovery					
	Service Execution	Hidden Files and Directories	Process Injection	HIDDEN	System Owner/User Discovery					
	Signed Binary Proxy Execution	Hypervisor	Scheduled Task	Image File Execution Options Injection	System Service Discovery					
	Signed Script Proxy Execution	Image File Execution Options Injection	Kernel Modules and Extensions	HISTCONTROL						
	Source	Launch Agent	Setuid and Setgid	Setuid and Setgid						
	Space after Filename									



n  
is  
nnels  
munication  
ption  
Tools  
y  
ation  
graphic  
pplication  
ed Port

# NIST Cybersecurity Framework (CSF)



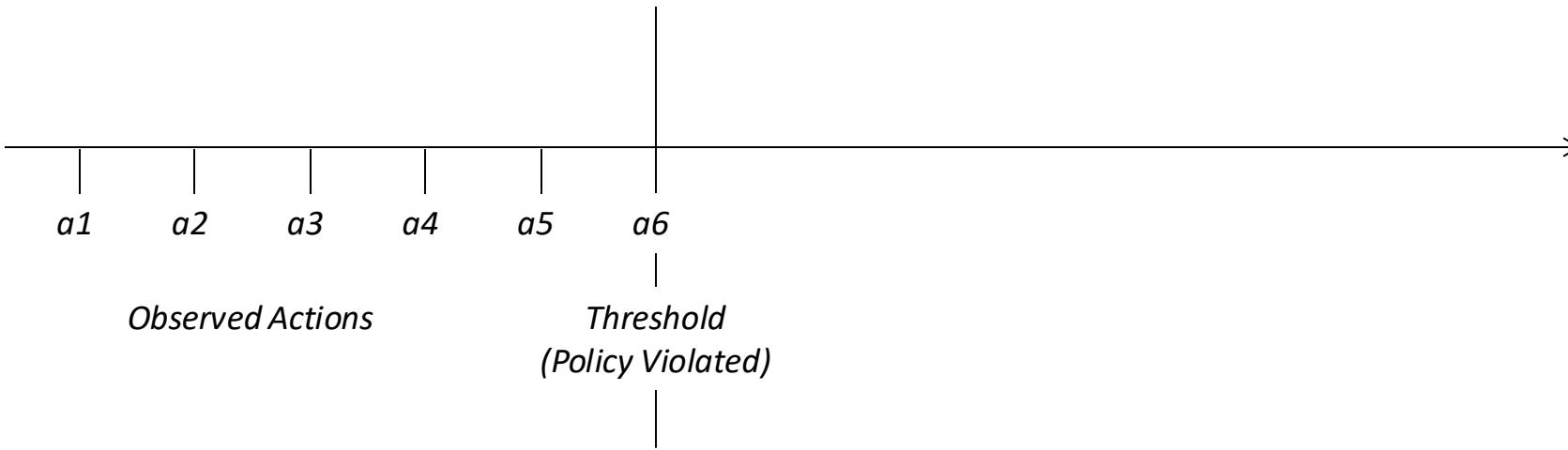
# NIST Cybersecurity Framework (CSF) – Version 2.0



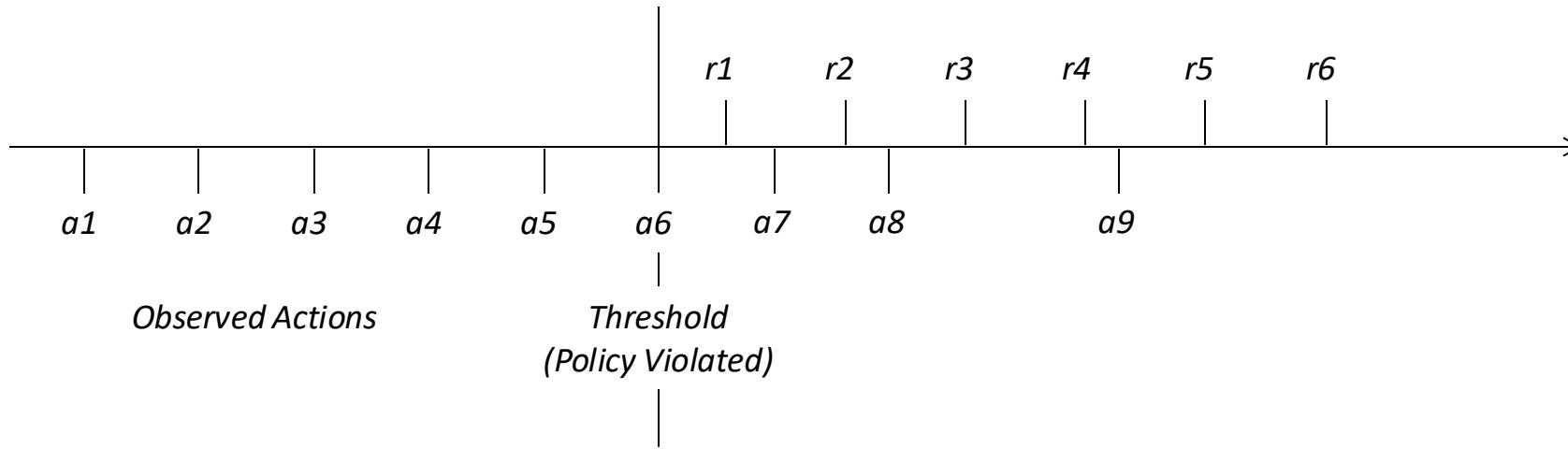
# Cyber Security: Attack Lifecycle (Defense View)



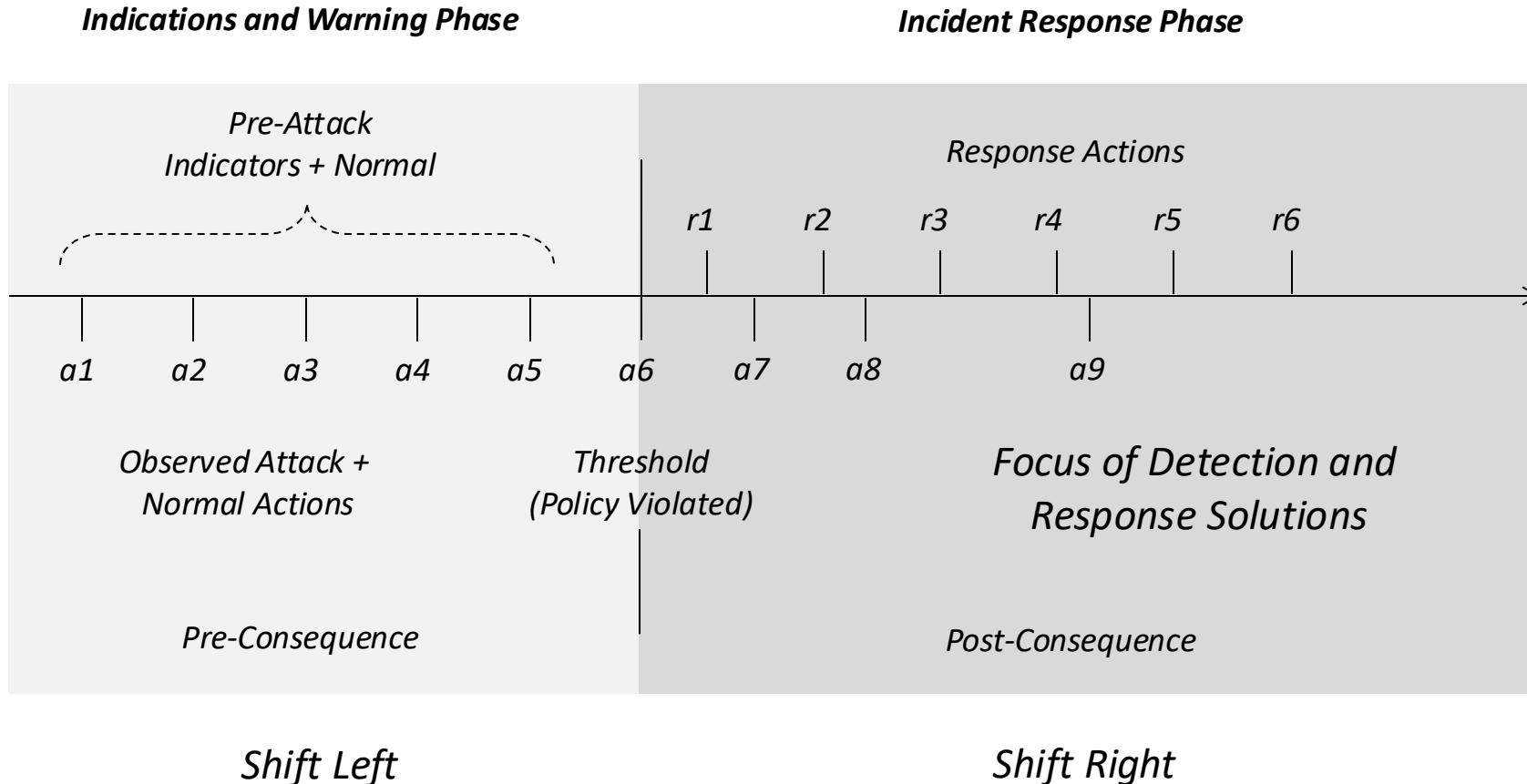
# Cyber Security: Attack Lifecycle (Defense View)



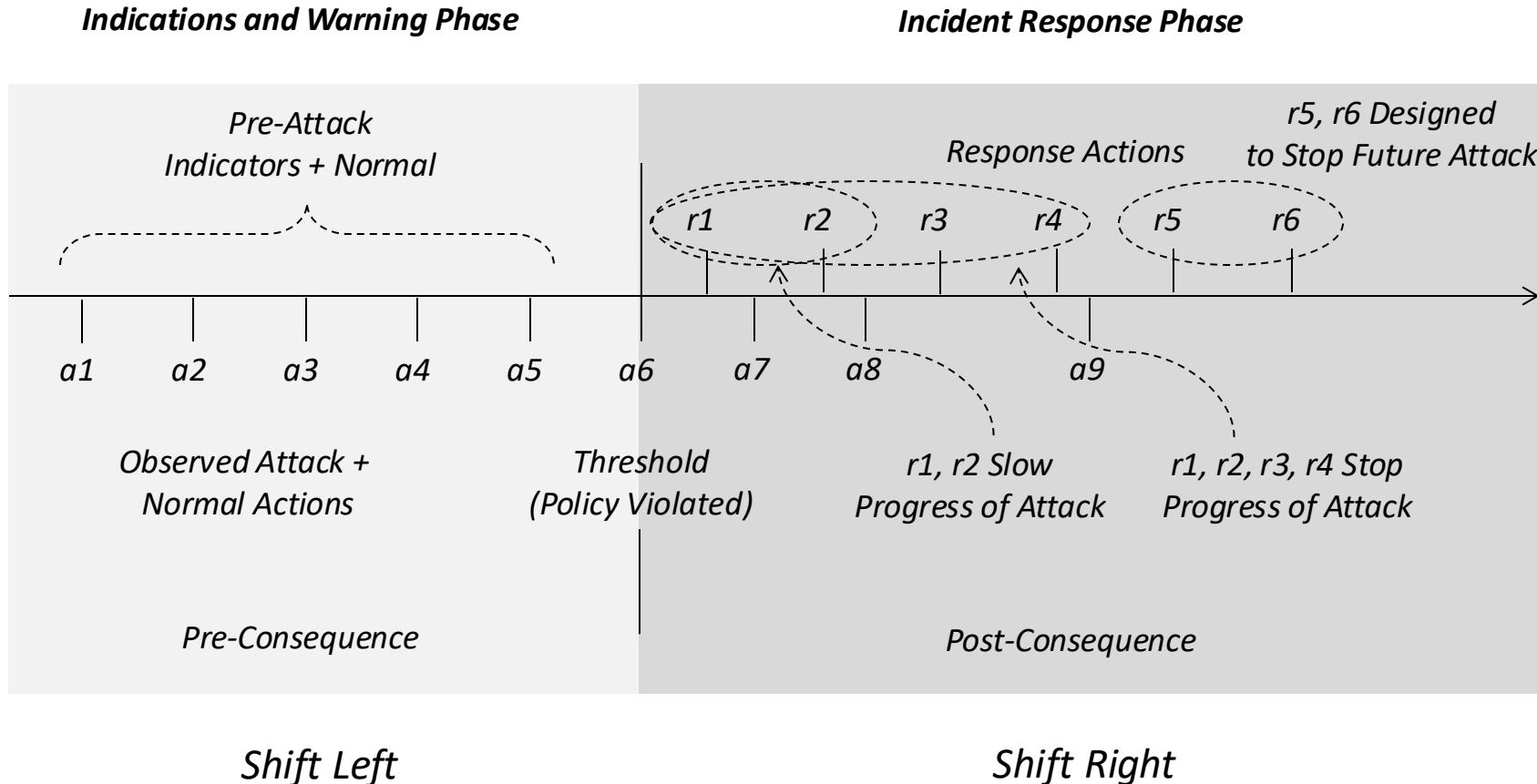
# Cyber Security: Attack Lifecycle (Defense View)



# Cyber Security: Attack Lifecycle (Defense View)



# Cyber Security: Attack Lifecycle (Defense View)



The image is a wide-angle aerial shot of a university campus. In the foreground, a large green football field with white yard lines and a red "S" logo is visible. To the left, there's a modern building with a glass facade and a dark roof. Behind the field, several older, multi-story brick buildings with white-framed windows are scattered among green trees. In the middle ground, a large body of water, likely the Hudson River, stretches across the frame. On the opposite bank, the dense urban skyline of New York City is visible, featuring numerous skyscrapers of varying heights under a clear blue sky.

# Course Requirements

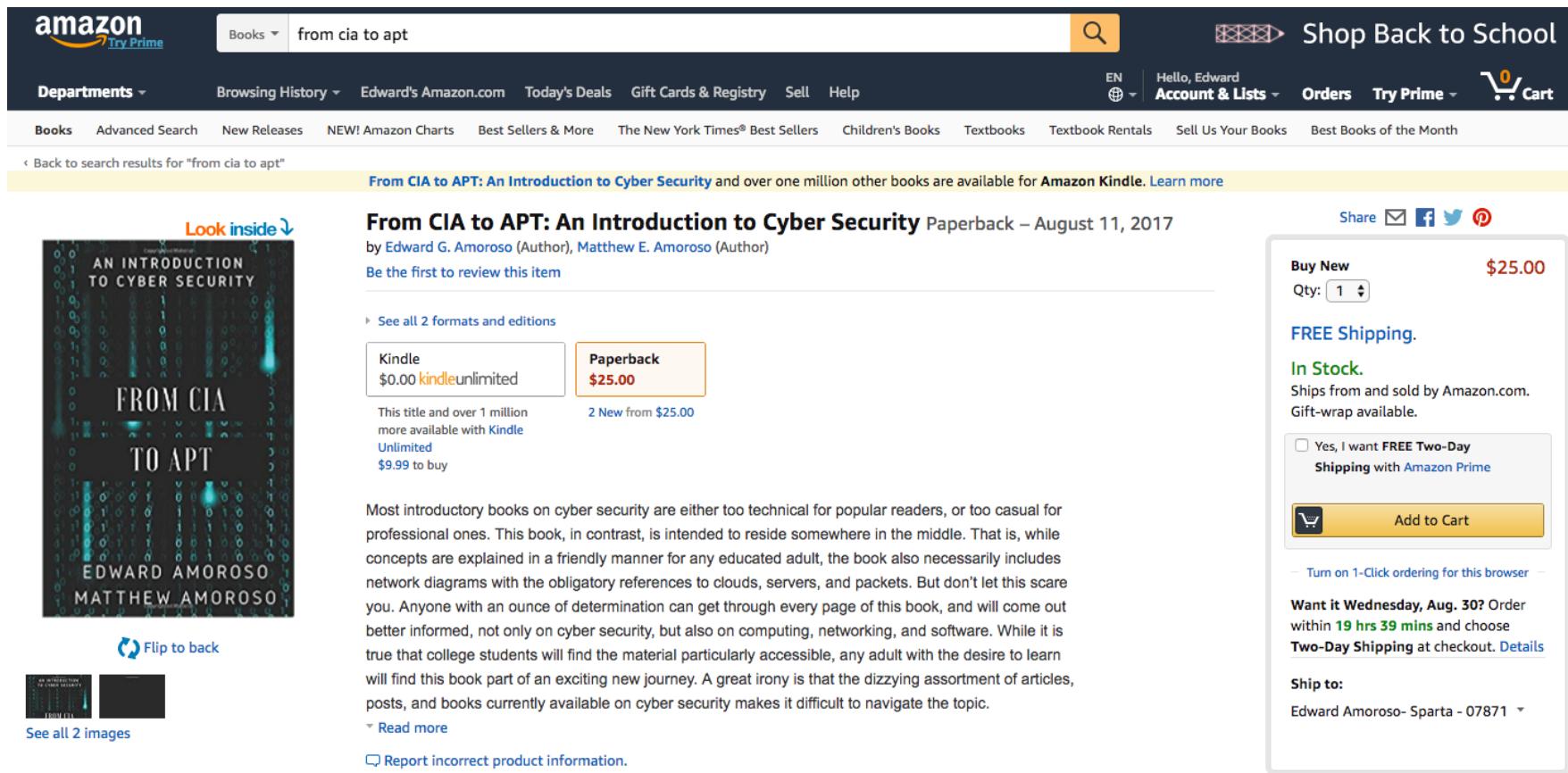
Midterm Project – 40%

Final Examination (In-Class) – 40%

Class Presence and Participation – 20%



# Required Text – \$9.99 Download from Amazon.com \$25.00 Printed Paperback Book from Amazon.com **From CIA to APT: An Introduction to Cyber Security** **Edward G. Amoroso & Matthew E. Amoroso**



The screenshot shows the Amazon product page for the book "From CIA to APT: An Introduction to Cyber Security". The page includes the book cover, a "Look inside" button, and a summary of the book's content. The price is listed as \$25.00 for the Paperback edition, which is available with Kindle Unlimited. The book is marked as being in stock with free shipping. The page also features social sharing options and a "Buy New" button.

**From CIA to APT: An Introduction to Cyber Security** Paperback – August 11, 2017

by Edward G. Amoroso (Author), Matthew E. Amoroso (Author)

Be the first to review this item

See all 2 formats and editions

Kindle  
\$0.00 kindleunlimited

Paperback  
\$25.00

This title and over 1 million more available with Kindle Unlimited  
\$9.99 to buy

2 New from \$25.00

Most introductory books on cyber security are either too technical for popular readers, or too casual for professional ones. This book, in contrast, is intended to reside somewhere in the middle. That is, while concepts are explained in a friendly manner for any educated adult, the book also necessarily includes network diagrams with the obligatory references to clouds, servers, and packets. But don't let this scare you. Anyone with an ounce of determination can get through every page of this book, and will come out better informed, not only on cyber security, but also on computing, networking, and software. While it is true that college students will find the material particularly accessible, any adult with the desire to learn will find this book part of an exciting new journey. A great irony is that the dizzying assortment of articles, posts, and books currently available on cyber security makes it difficult to navigate the topic.

Read more

Report incorrect product information.

Buy New \$25.00

Qty: 1

FREE Shipping.

In Stock.

Ships from and sold by Amazon.com. Gift-wrap available.

Yes, I want FREE Two-Day Shipping with Amazon Prime

Add to Cart

Turn on 1-Click ordering for this browser

Want it Wednesday, Aug. 30? Order within 19 hrs 39 mins and choose Two-Day Shipping at checkout. Details

Ship to:

Edward Amoroso- Sparta - 07871