An Introduction to Cyber Security – CS 573

Instructor: Dr. Edward G. Amoroso
eamoroso@tag-cyber.com

Week 1

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-actuated computer systems.

Week 1

2023


I'm...
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in
ChatGPT
Regenerate response
Dark Mode
Updates
Log out


Week 1
verizon

Week 1


Week 1
verizon


Week 1

Week 1

cebook

Email or Phone: eamoroso@att.net

Password: ••••••••

Log In

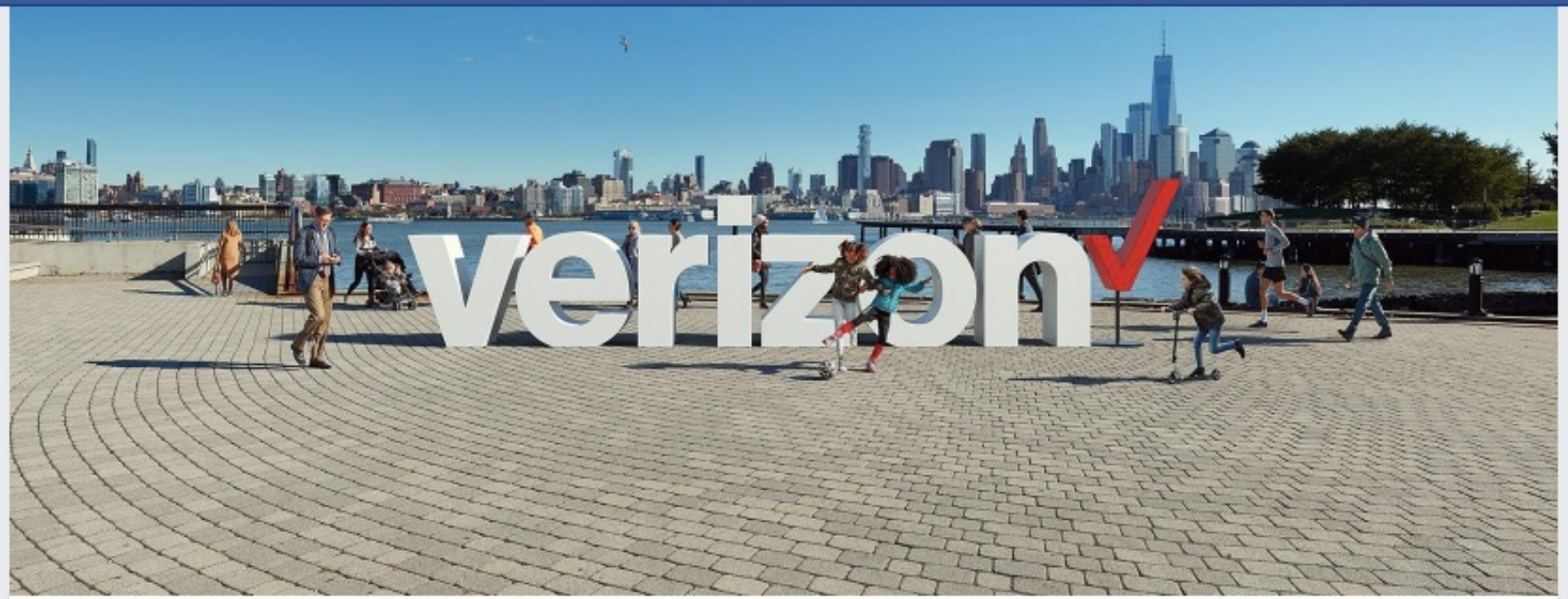
Forgot account?

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

7,079,897 people follow this

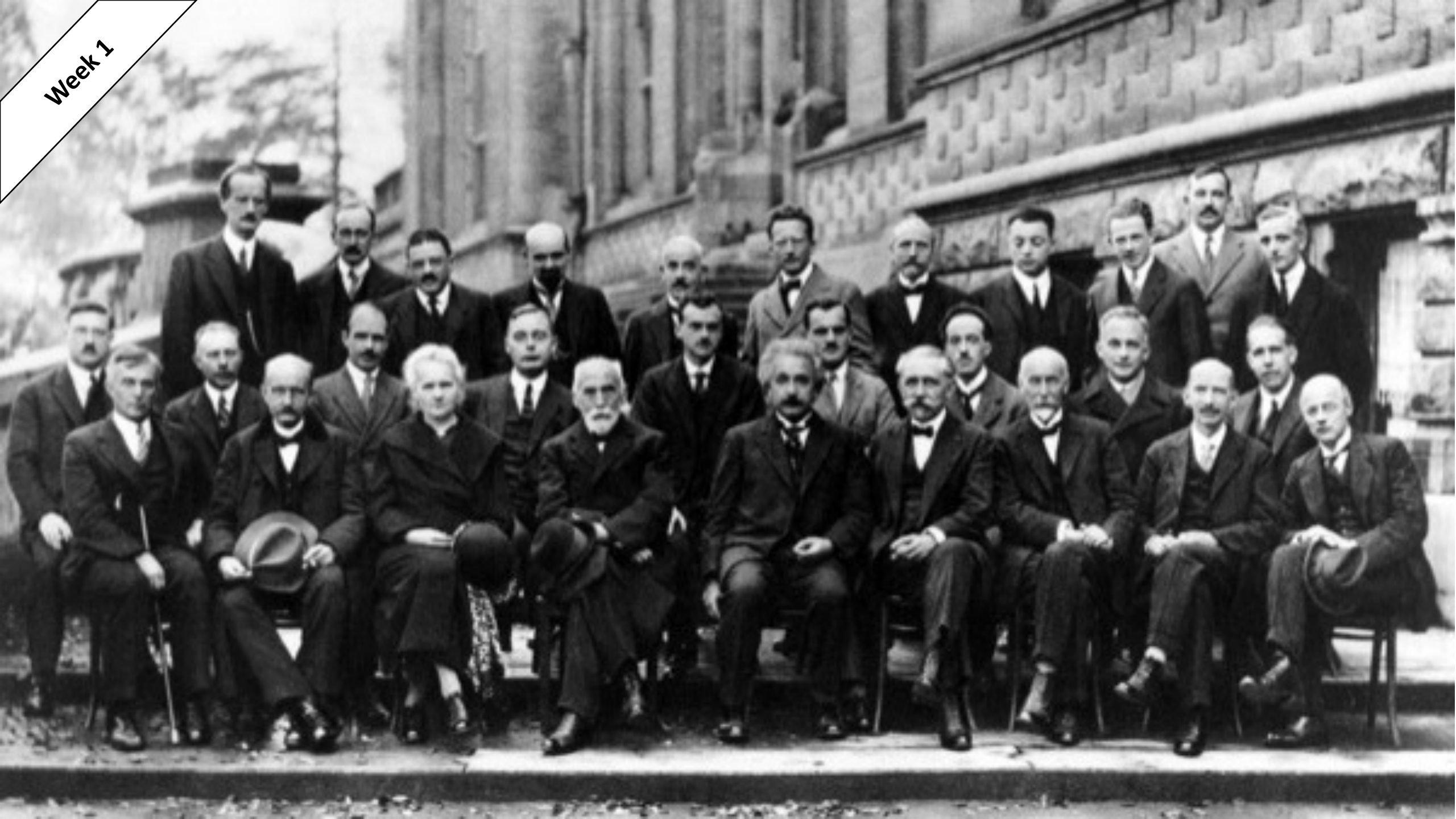
About See All

See more of Verizon on Facebook

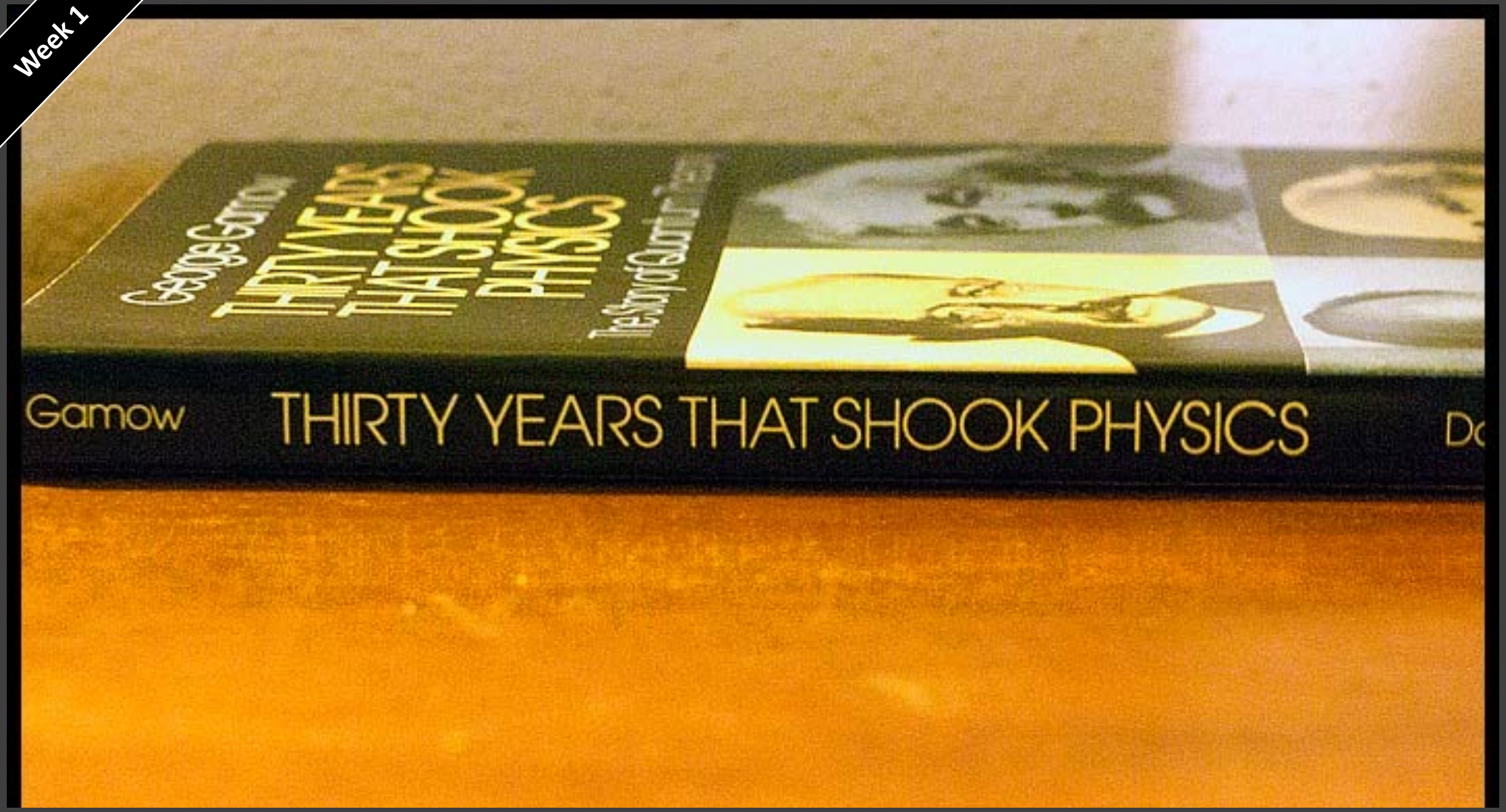
Week 1: Introduction to Cyber Security Issues

How Does Invention (Innovation) Affect Security?

Week 1



Week 1


George Gamow
THE STORY OF MODERN PHYSICS
Gamow
THIRTY YEARS THAT SHOOK PHYSICS

Week 1

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. Now 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.

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 inofficial 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.

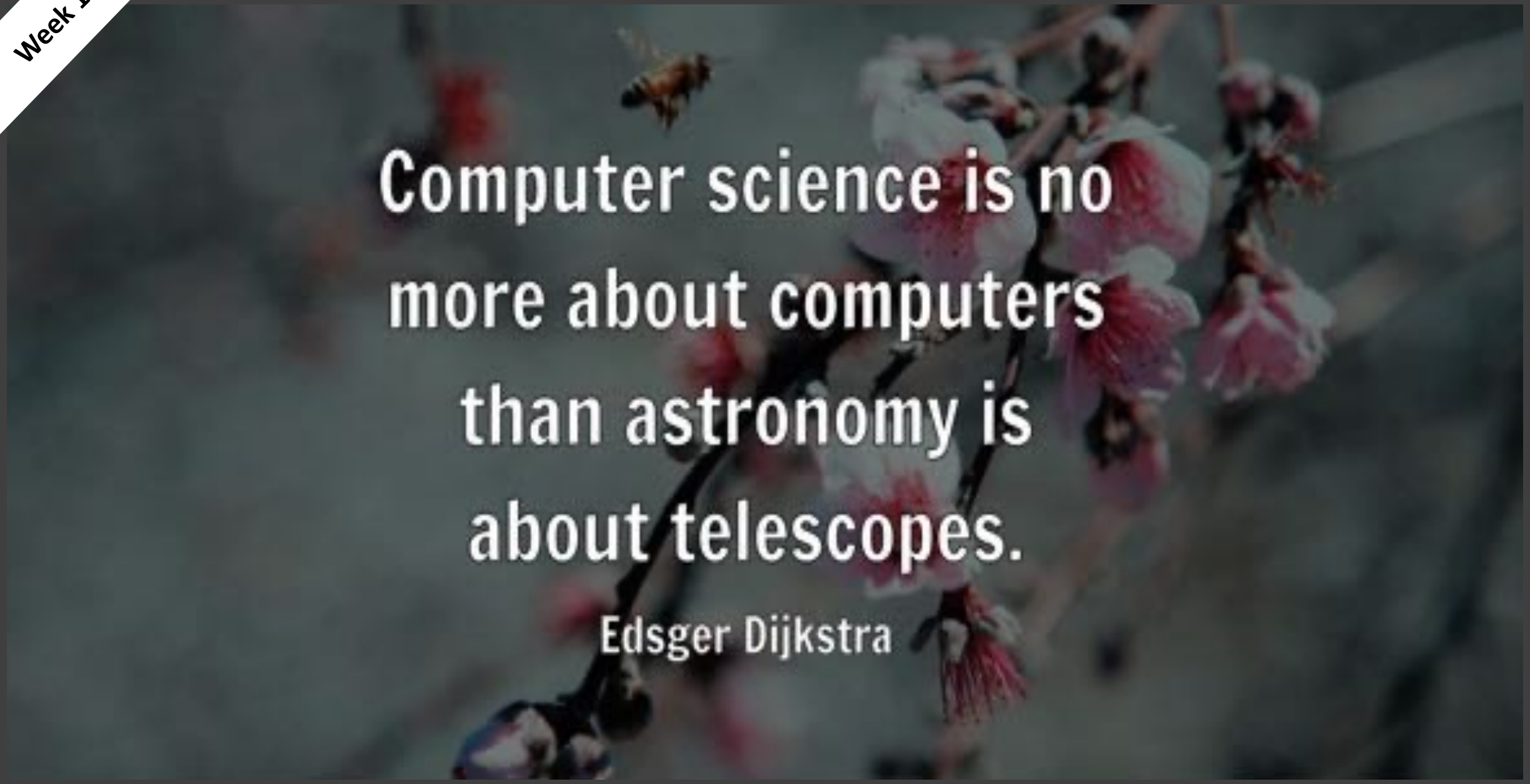
Yours very truly,

A. Einstein

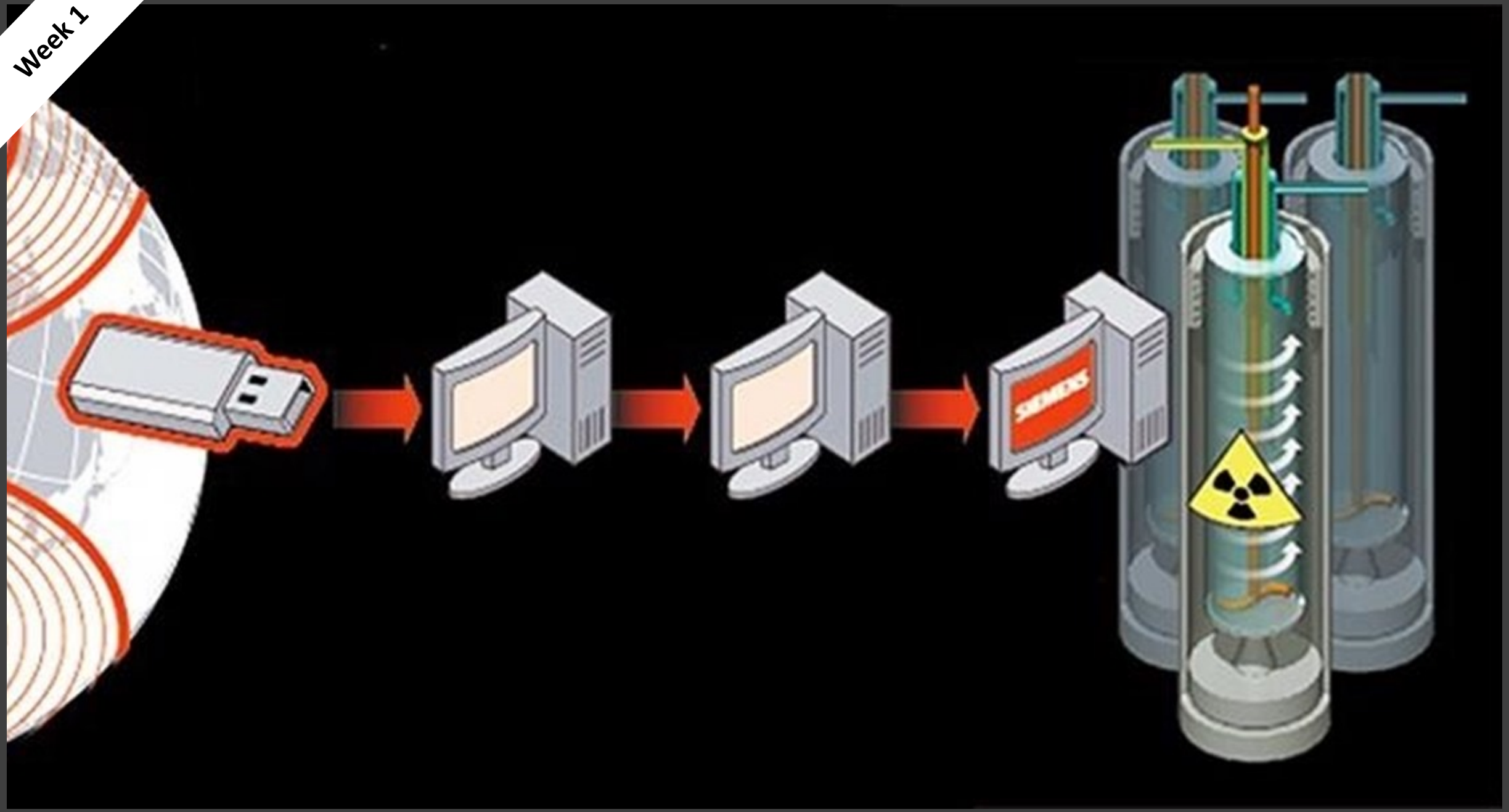
(Albert Einstein)

Week 1

Week 1


Computer science is no more about computers than astronomy is about telescopes.
Edsger Dijkstra

Week 1



Week 1

EA

Did computer scientists from 1968 to 2008 change the world more than physicists from 1890 to 1930?

It is difficult to compare the impact of computer scientists from 1968 to 2008 to the impact of physicists from 1890 to 1930, as they have contributed to different fields and have had different levels of impact. Both groups have made significant contributions to their respective fields and have had a significant impact on the world. It is not possible to say which group has had a greater impact without further context and information.

Does Government Understand Cybersecurity?

Week 1

Week 1

Protecting Critical Assets (National Infrastructure) – 1998

Week 1

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

Week 1

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

What are the Most Capable Nation-State Offense?

Week 1

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

1.
2.
3.
4.
5.

Week 1

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

1. US
2.
3.
4.
5.

Week 1

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

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

Week 1

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.

Week 1

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.

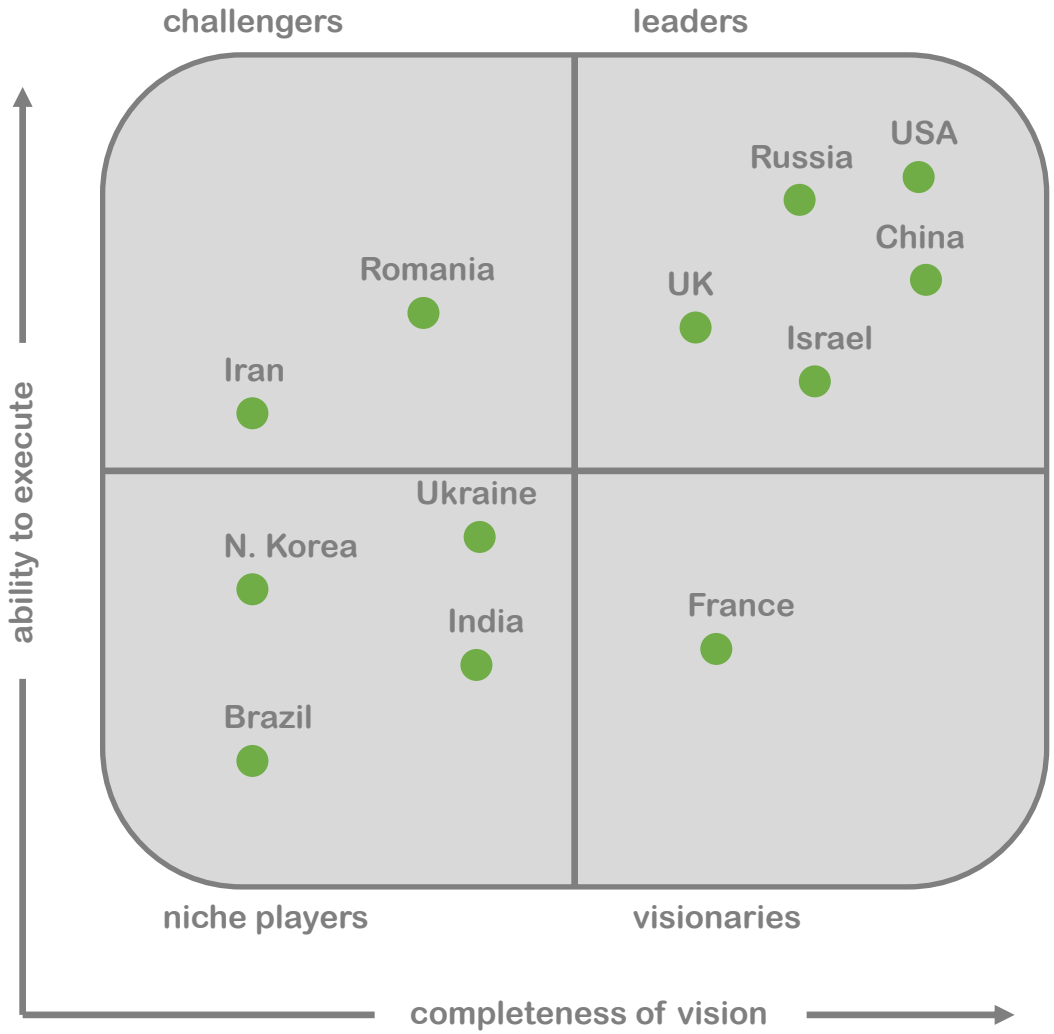
Week 1

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

Week 1

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

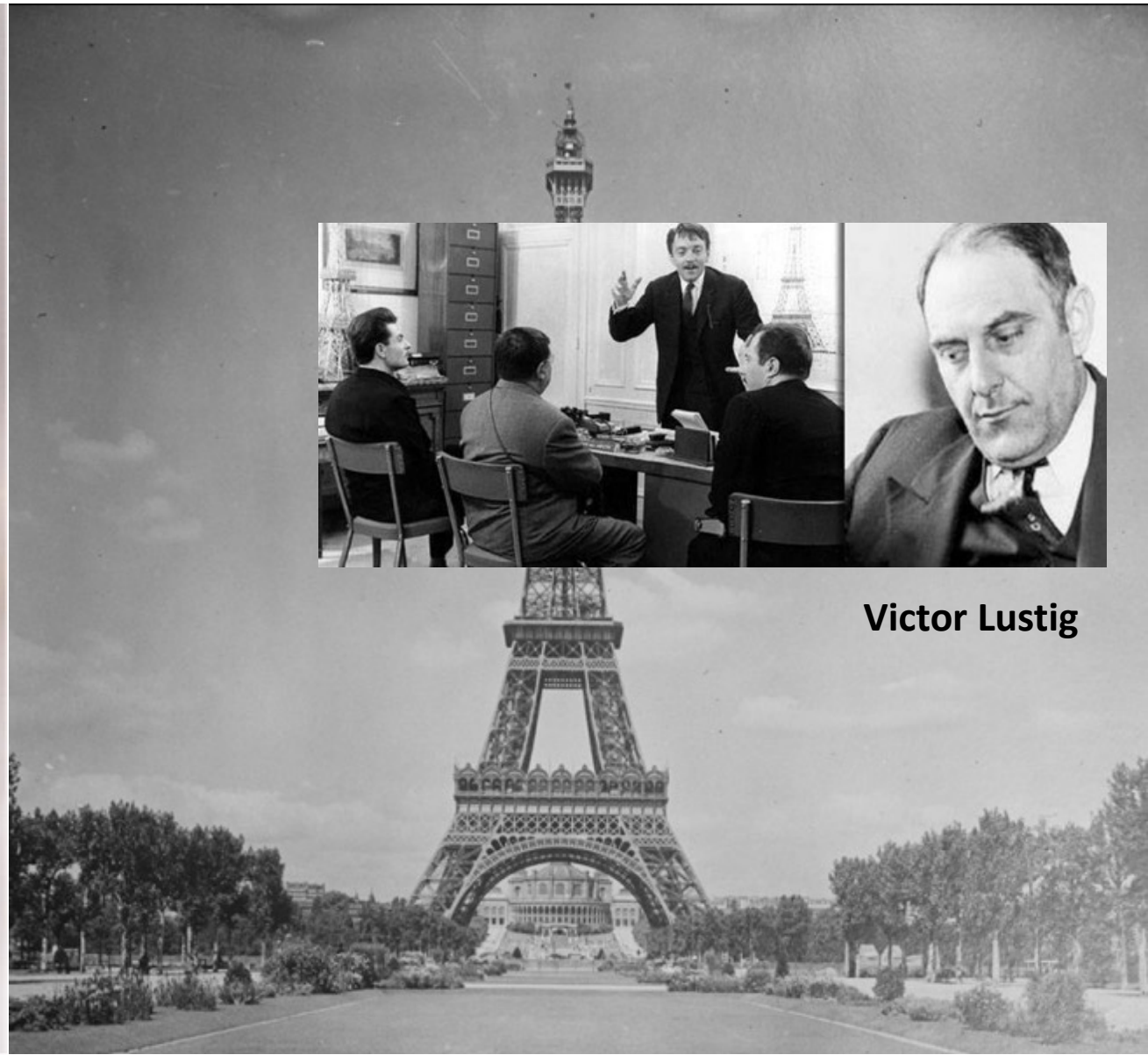
What Can Be Learned from the Earliest Hacks?

Week 1

Understanding the Hack: 70's Vintage Soda Machine

Week 1

Understanding the Hack: Early Scams and Social Engineering



Week 1

Understanding the Hack: Unauthorized Infrastructure Access

KIIS FM 102.7

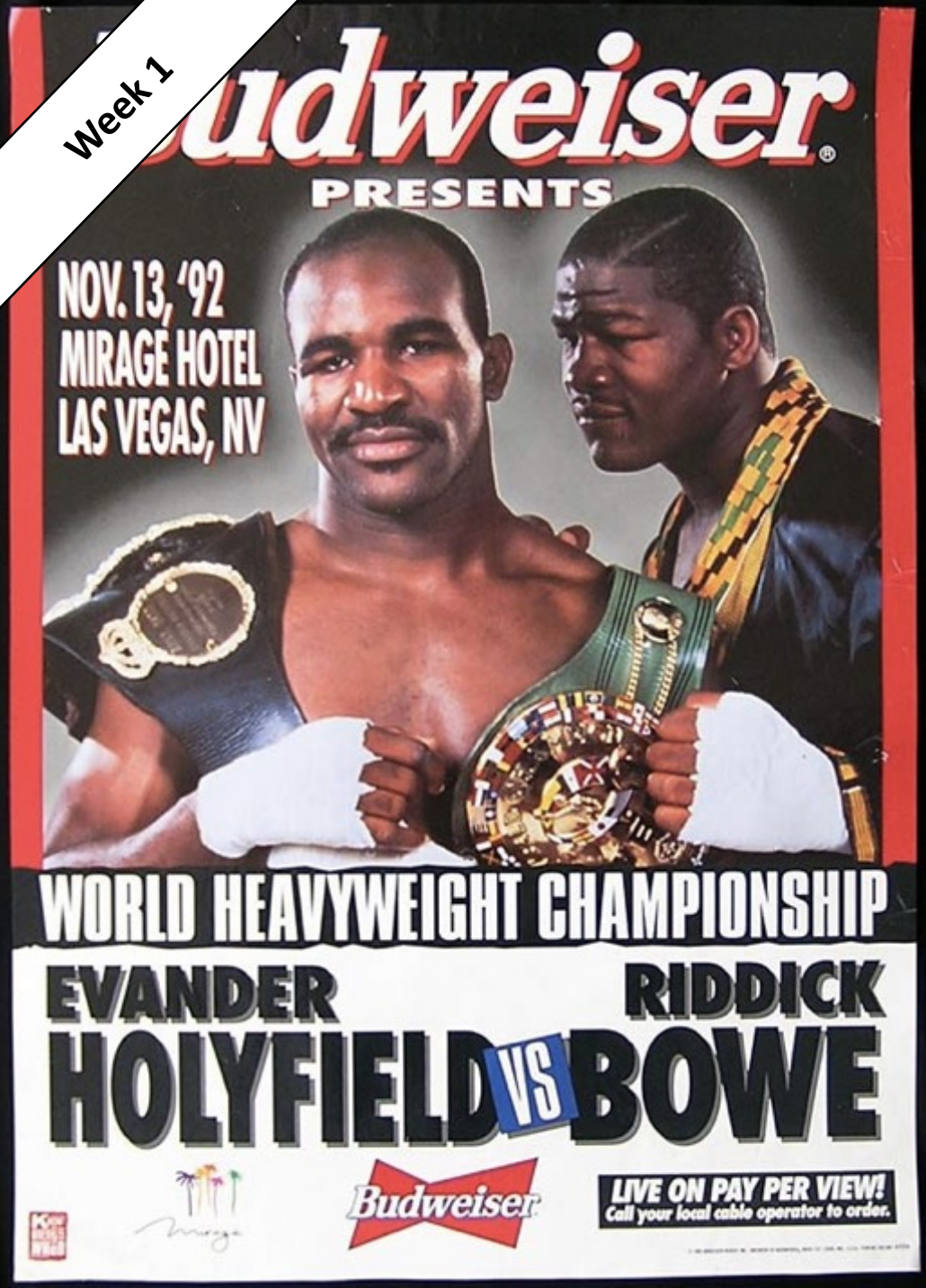
RICK DEES
IN THE MORNING

AUGUST 18, 1990

PACIFIC BELL

Kevin Poulsen

Week 1

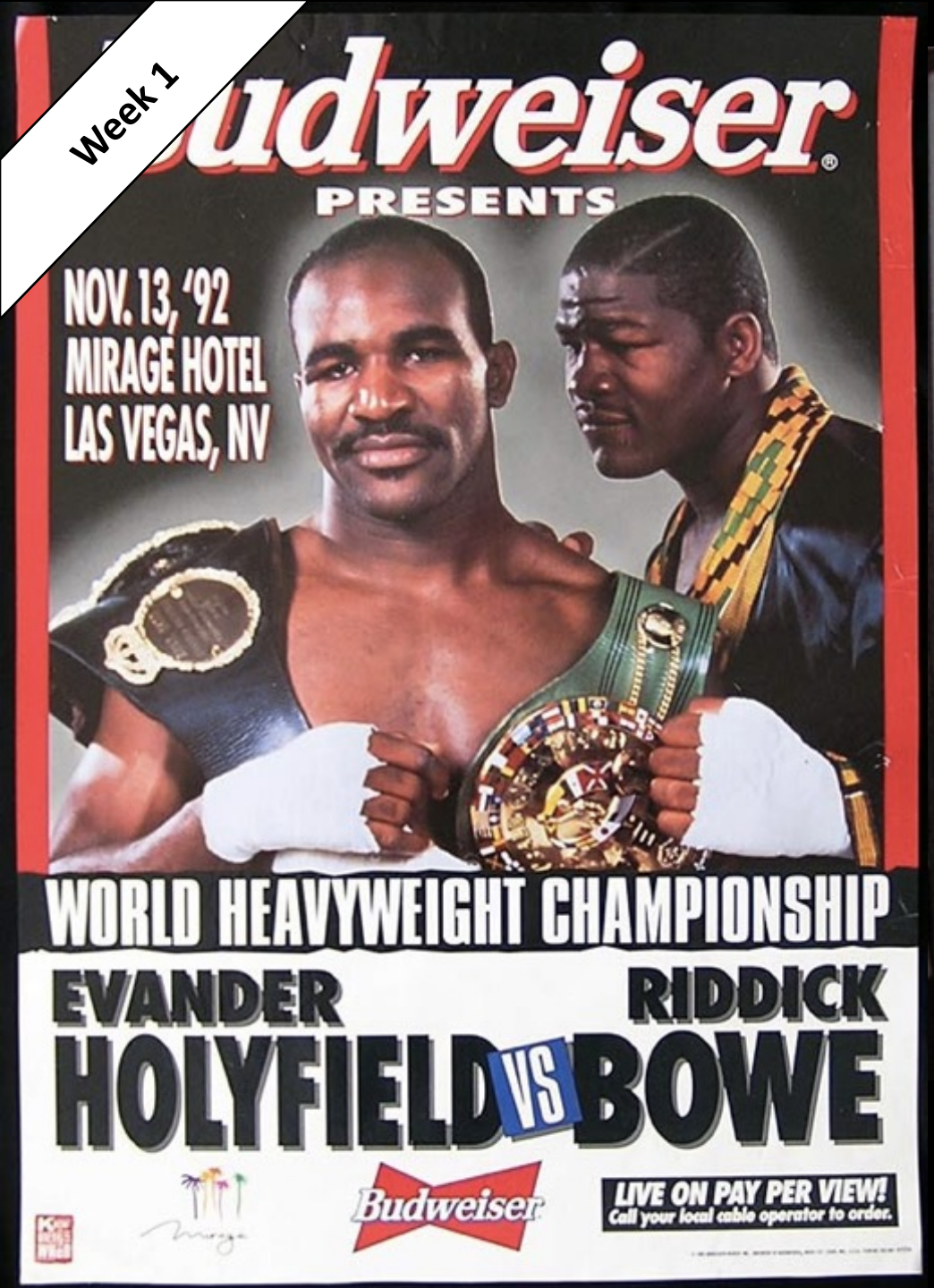


Scrambled Picture for Non-Payers

Week 1

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]

Week 1



Fake Enticement for Fraudsters

How Do We Model Attack Strategy?

Week 1

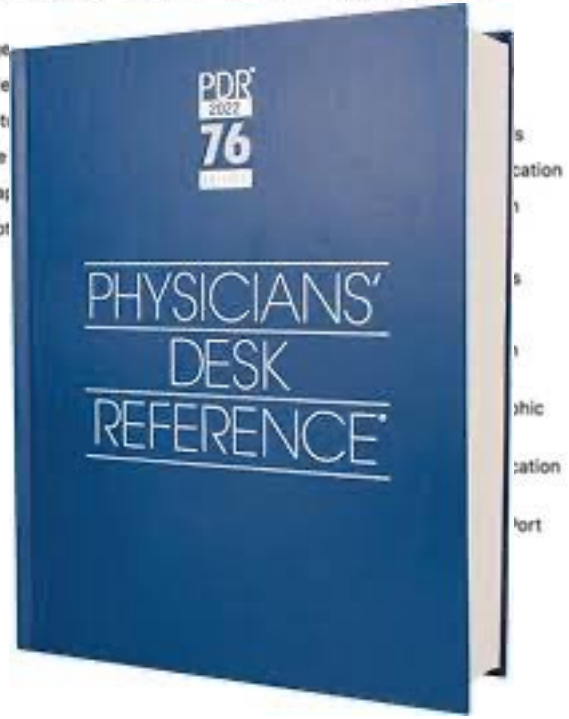
MITRE ATT&CK Framework

ial 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	File and Directory Discovery	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 Files	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Process Discovery	Remote Services	Input Capture		Multi-hop Proxy
	Launchctl	Component Firmware	File System Permissions Weakness	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Local Job Scheduling	Component Object Model Hijacking	Hooking	Deobfuscate/Decode Files or Information	Kerberoasting	Remote System Discovery	Shared Webroot	Screen Capture		Multiband Communication
	LSASS Driver	Create Account	Image File Execution Options Injection	Disabling Security Tools	Keychain	Security Software Discovery	SSH Hijacking	Video Capture		Multilayer Encryption
	Mshta	DLL Search Order Hijacking	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	System Information Discovery	Taint Shared Content			Port Knocking
	PowerShell	Dylib Hijacking	New Service	DLL Side-Loading	Network Sniffing	System Network Configuration Discovery	Third-party Software			Remote Access Tools
	Regsvcs/Regasm	External Remote Services	Path Interception	Exploitation for Defense Evasion	Password Filter DLL	System Network Connections Discovery	Windows Admin Shares			Remote File Copy
	Regsvr32	File System Permissions Weakness	Plist Modification	Extra Window Memory Injection	Private Keys	System Owner/User Discovery	Windows Remote Management			Standard Application Layer Protocol
	Rundll32	Hidden Files and Directories	Port Monitors	File Deletion	Replication Through Removable Media	System Service Discovery				Standard Cryptographic Protocol
	Scheduled Task	Hooking	Process Injection	File System Logical Offsets	Securityd Memory					Standard Non-Application Layer Protocol
	Scripting	Hypervisor	Scheduled Task	Gatekeeper Bypass	Two-Factor Authentication Interception					Uncommonly Used Port
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	Hidden Files and Directories						Web Service
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	Hidden Users						
	Signed Script Proxy Execution	Launch Agent		Hidden Window						
	Source			HISTCONTROL						
	Space after Filename			Image File Execution Options Injection						

Week 1

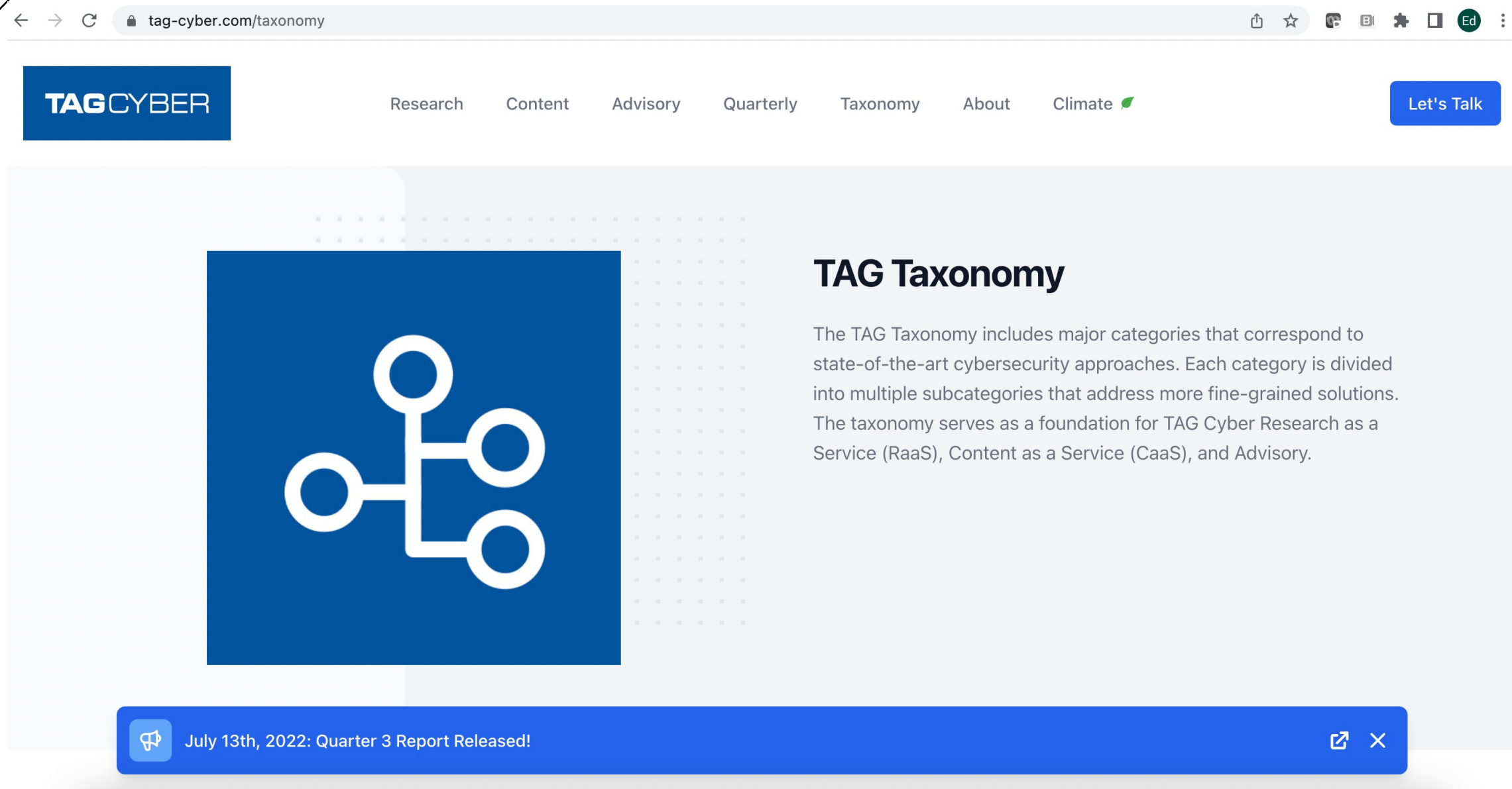
MITRE ATT&CK Framework

ial 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	File and Directory Discovery	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 Files	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Removable Media		Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data Staged		
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy	Email Collection		
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Process Discovery	Remote Services	Input Capture		
	Launchctl	Component Firmware	File System Permissions Weakness	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser		
	Local Job Scheduling	Component Object Model Hijacking	Hooking	Deobfuscate/Decode Files or Information	Kerberoasting	Remote System Discovery	Shared Webroot	Screen Capture		
	LSASS Driver	Create Account	Image File Execution Options Injection	Disabling Security Tools	Keychain	Security Software Discovery	SSH Hijacking	Video Capture		
	Mshta	DLL Search Order Hijacking	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	System Information Discovery	Taint Shared Content			
	PowerShell	Dylib Hijacking	New Service	DLL Side-Loading	Network Sniffing	System Network Configuration Discovery	Third-party Software			
	Regsvcs/Regasm	External Remote Services	Path Interception	Exploitation for Defense Evasion	Password Filter DLL	System Network Connections Discovery	Windows Admin Shares			
	Regsvr32	File System Permissions Weakness	Plist Modification	Extra Window Memory Injection	Private Keys	System Owner/User Discovery	Windows Remote Management			
	Rundll32	Hidden Files and Directories	Port Monitors	File Deletion	Replication Through Removable Media	System Service Discovery				
	Scheduled Task	Hooking	Process Injection	File System Logical Offsets	Securityd Memory					
	Scripting	Hypervisor	Scheduled Task	Gatekeeper Bypass	Two-Factor Authentication Interception					
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	Hidden Files and Directories						
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	Hidden Users						
	Signed Script Proxy Execution	Launch Agent		Hidden Window						
	Source			HISTCONTROL						
	Space after Filename			Image File Execution Options Injection						



Week 1

TAG Cyber Taxonomy – Commercial Platforms



Week 1

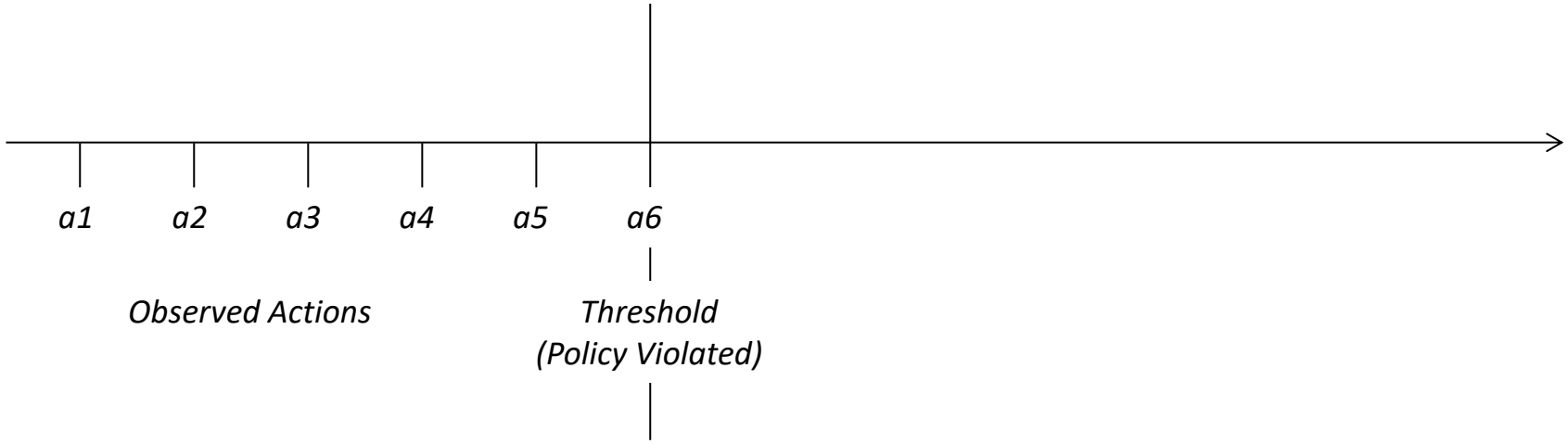
NIST Cybersecurity Framework (CSF)

Week 1

Cyber Security: Attack Lifecycle (Defense View)

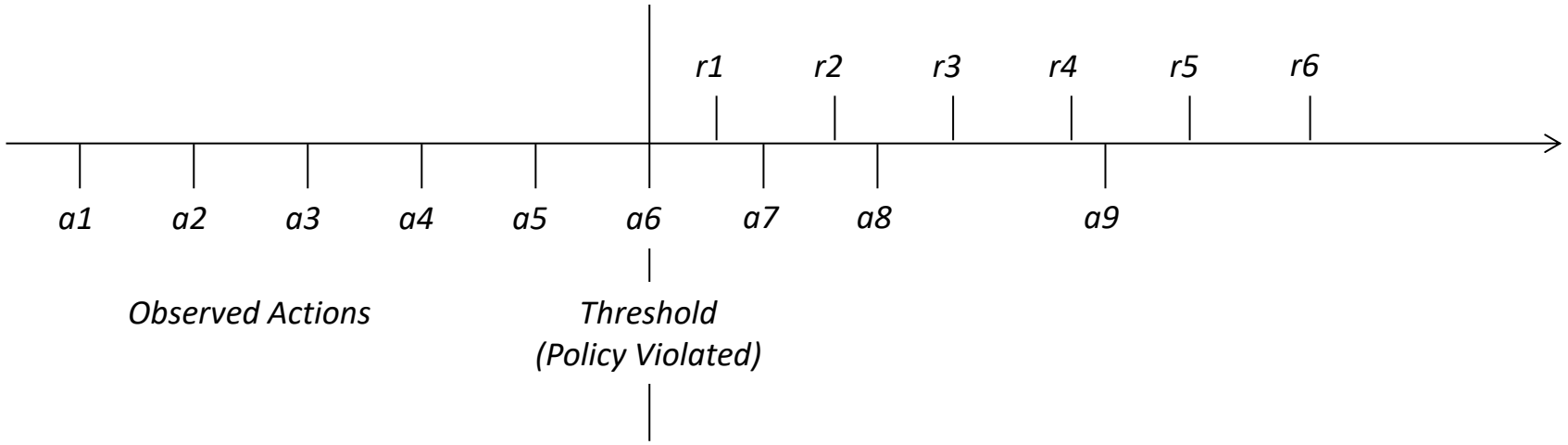
Week 1

Cyber Security: Attack Lifecycle (Defense View)



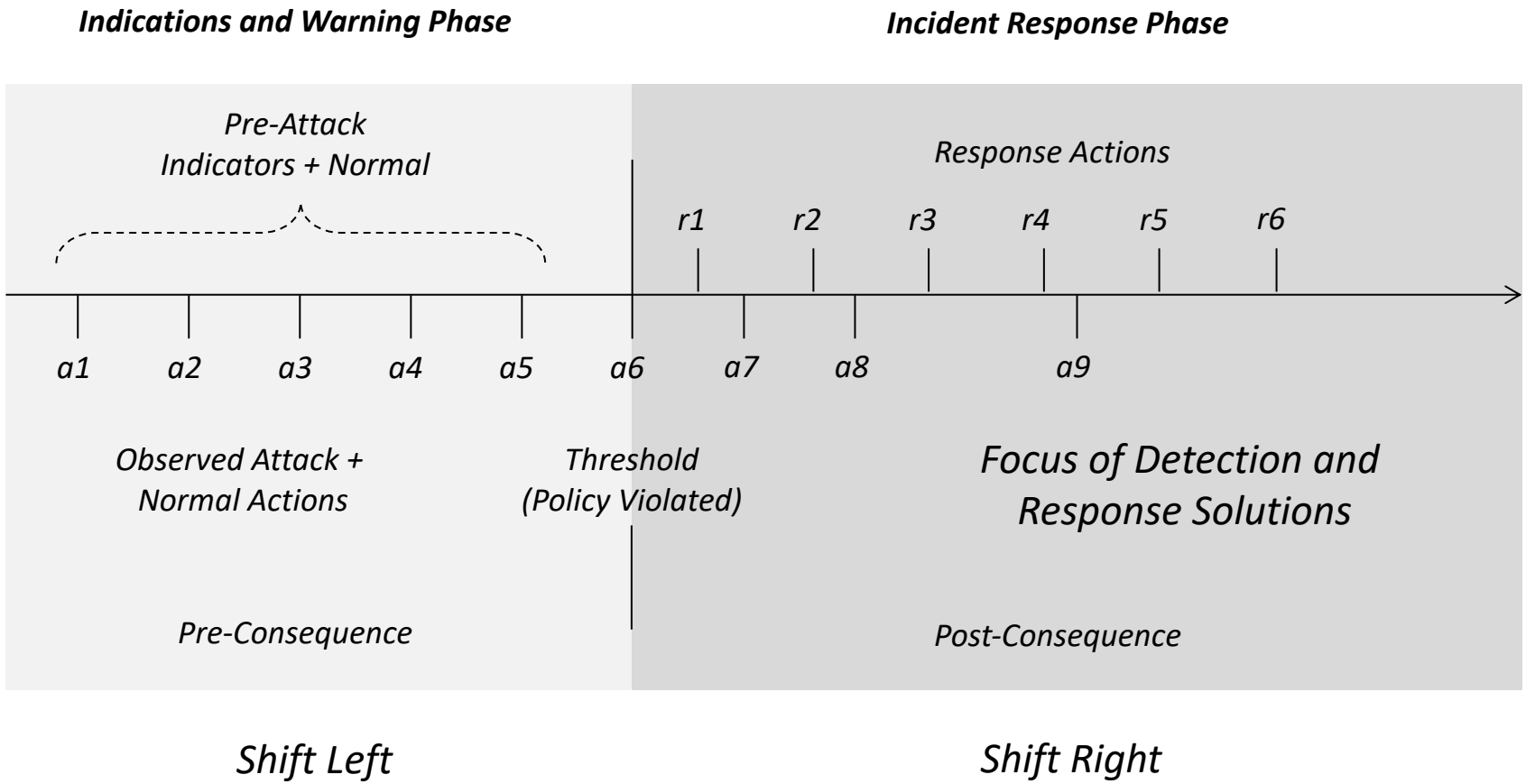
Week 1

Cyber Security: Attack Lifecycle (Defense View)



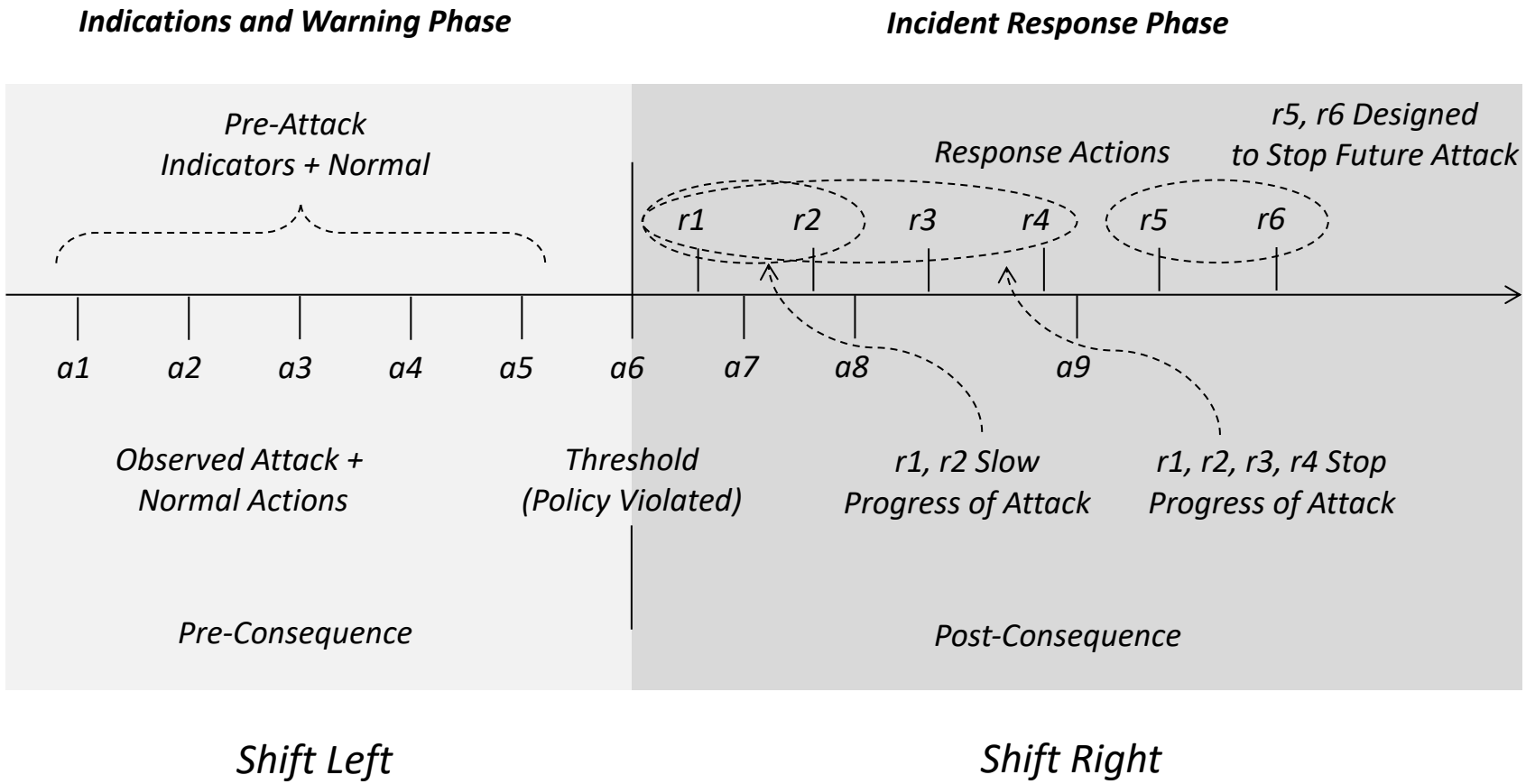
Week 1

Cyber Security: Attack Lifecycle (Defense View)



Week 1

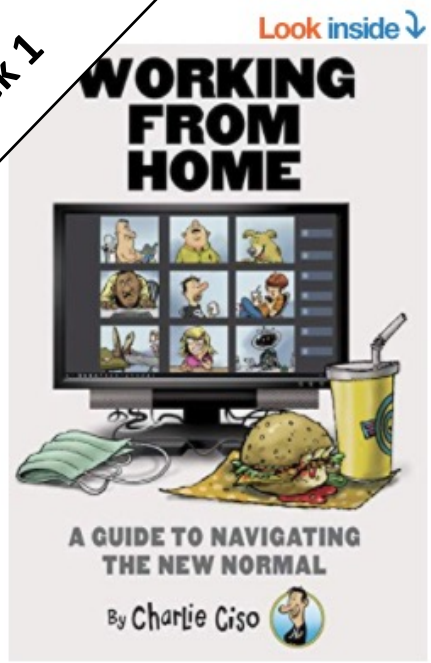
Cyber Security: Attack Lifecycle (Defense View)



Week 1

Charlie CISO Cartoons (Follow Edward Amoroso on LinkedIn)

Week 1



Working from Home: A Guide to Navigating the New Normal

Kindle Edition

by Edward Amoroso (Author), Rich Powell (Author) | Format: Kindle Edition

★★★★★ 16 ratings

› See all formats and editions

Kindle
$4.99

Read with Our Free App

If you are in need of some Pandemic entertainment and world-class comic relief, then "Working from Home: A Guide to Navigating the New Normal" is for you! This step-by-step guide, written by a fictitious social media sensation (and sometimes cybersecurity expert) named Charlie Ciso, will teach you to:

•Build a fake Zoom backdrop that will get you promoted to senior VP in ten days or less

‹ Read more

Kindle Price: $4.99

Read Now

You already own this item. Read anytime on your Kindle apps and devices.

Buy for others

Give as a gift or purchase for a team or group. Learn more

Quantity: 1 Buy for others

Add to List

Enter a promotion code or Gift Card

Share <Embed>

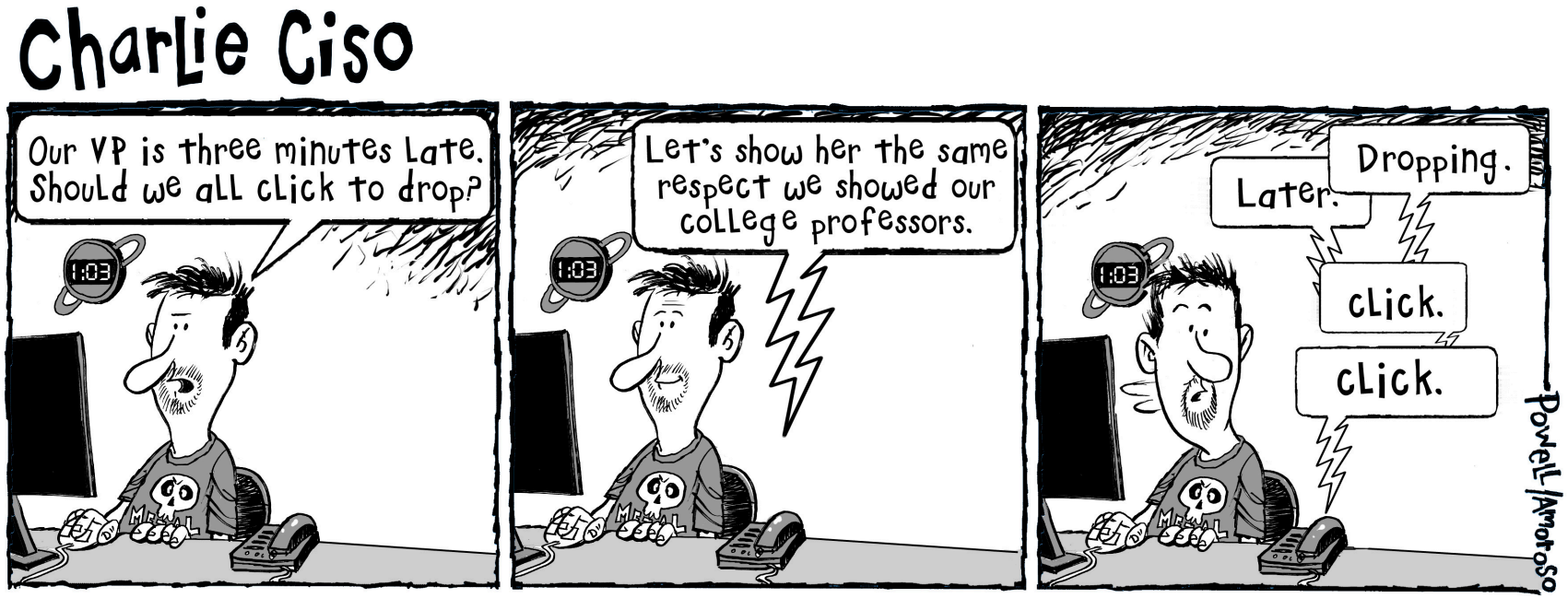
Follow the Author

Edward G. Amoroso

+ Fol

READ ON ANY DEVICE

›Get free Kindle app



Week 1

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

Week 1

Required Week One Readings

1. "Reflections on Trusting Trust," Ken Thompson
https://www.ece.cmu.edu/~ganger/712.fall02/papers/p761-thompson.pdf

2. **Chapters 1 through 4: *From CIA to APT: An Introduction to Cyber Security*, E. Amoroso & M. Amoroso**

Twitter: @hashtag_cyber
LinkedIn: Edward Amoroso