Winning the Cyber War: Good vs Evil

Dr. Dalia Khader

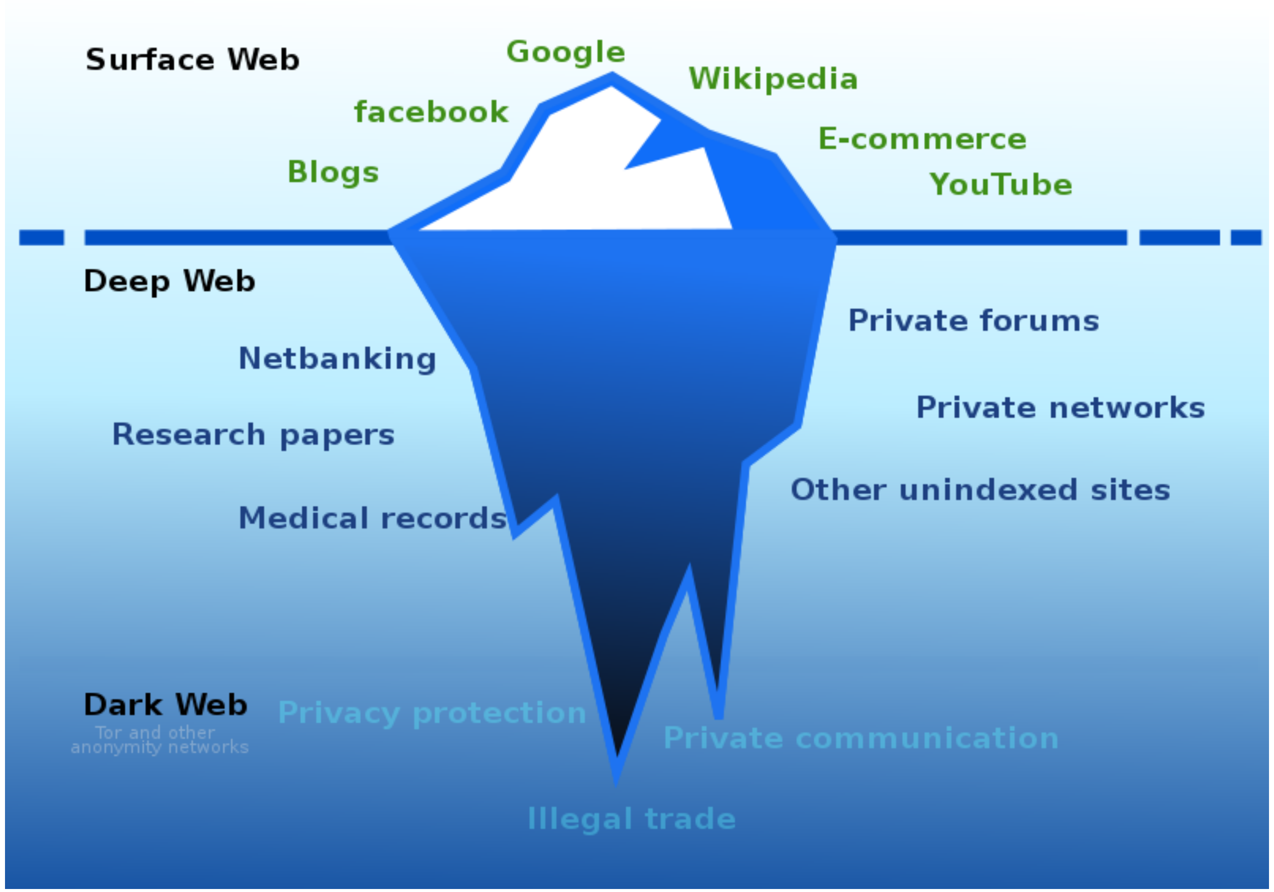
Who Am I?

- More than 15 years of experience in the domain of information security.
- CISO of Swiss Life International Division, an insurance company that focuses on private wealth and employee benefits.
- Started my career as a researcher in Cryptography and did a good amount of teaching during that period.
- Proud member of Cyber Force Woman
- Winner of CISO 2021 Award, Luxembourg

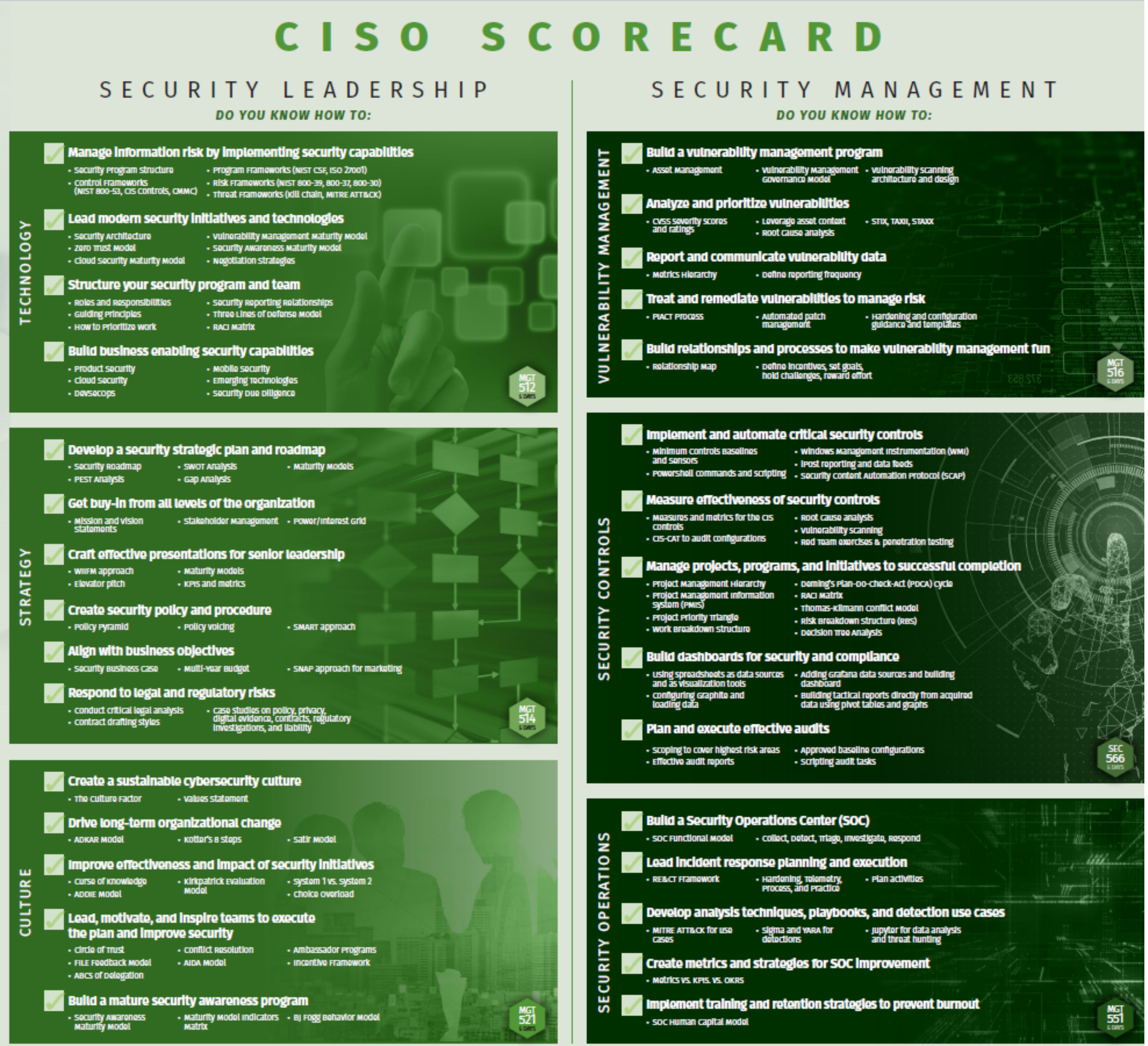
Demystifying the Dark Web

SANS.ORG The Dark Web consists of systems on the Internet designed for communicating or sharing information securely and anonymously. The Dark Web is collections of different systems and networks managed by different people used for a variety of purposes. These systems are still connected to and are part of the Internet; however, you will generally not find them using your normal search engines. You often also need special software on your computer to find or access them.

Wikipedia The dark web is the World Wide Web content that exists on darknets: overlay networks that use the Internet but require specific software, configurations, or authorization to access. Through the dark web, private computer networks can communicate and conduct business anonymously without divulging identifying information, such as a user's location. The dark web forms a small part of the deep web, the part of the Web not indexed by web search engines, although sometimes the term deep web is mistakenly used to refer specifically to the dark web. The darknets which constitute the dark web include small, friend-to-friend peer-to-peer networks, as well as large, popular networks such as Tor, Freenet, I2P, and Riffle software operated by public organizations and individuals.



Wikimedia



CISO SCORECARD

SECURITY LEADERSHIP

DO YOU KNOW HOW TO:

TECHNOLOGY

☑ **Manage information risk by implementing security capabilities**
- Security Program Structure
- Control Frameworks (NIST 800-53, CIS Controls, CMMC)
- Program Frameworks (NIST CSF, ISO 27001)
- Risk Frameworks (NIST 800-39, 800-37, 800-30)
- Threat Frameworks (Kill Chain, MITRE ATT&CK)

☑ **Lead modern security initiatives and technologies**
- Security Architecture
- Zero Trust Model
- Cloud Security Maturity Model
- Vulnerability Management Maturity Model
- Security Awareness Maturity Model
- Negotiation Strategies

☑ **Structure your security program and team**
- Roles and Responsibilities
- Guiding Principles
- How to Prioritize Work
- Security Reporting Relationships
- Three Lines of Defense Model
- RACI Matrix

☑ **Build business enabling security capabilities**
- Product Security
- Cloud Security
- DevSecOps
- Mobile Security
- Emerging Technologies
- Security Due Diligence

MGT 512 5 DAYS

STRATEGY

☑ **Develop a security strategic plan and roadmap**
- Security Roadmap
- PEST Analysis
- SWOT Analysis
- Gap Analysis
- Maturity Models

☑ **Get buy-in from all levels of the organization**
- Mission and Vision Statements
- Stakeholder Management
- Power/Interest Grid

☑ **Craft effective presentations for senior leadership**
- WIIFM approach
- Elevator pitch
- Maturity Models
- KPIs and metrics

☑ **Create security policy and procedure**
- Policy Pyramid
- Policy Voicing
- SMART approach

☑ **Align with business objectives**
- Security Business Case
- Multi-Year Budget
- SNAP approach for marketing

☑ **Respond to legal and regulatory risks**
- Conduct critical legal analysis
- Contract drafting styles
- Case studies on policy, privacy, digital evidence, contracts, regulatory investigations, and liability

MGT 514 5 DAYS

CULTURE

☑ **Create a sustainable cybersecurity culture**
- The Culture Factor
- Values Statement

☑ **Drive long-term organizational change**
- ADKAR Model
- Kotter's 8 Steps
- Satir Model

☑ **Improve effectiveness and impact of security initiatives**
- Curse of Knowledge
- ADDIE Model
- Kirkpatrick Evaluation Model
- System 1 vs. System 2
- Choice Overload

☑ **Lead, motivate, and inspire teams to execute the plan and improve security**
- Circle of Trust
- FILE Feedback Model
- ABCs of Delegation
- Conflict Resolution
- AIDA Model
- Ambassador Programs
- Incentive Framework

☑ **Build a mature security awareness program**
- Security Awareness Maturity Model
- Maturity Model Indicators Matrix
- BJ Fogg Behavior Model

MGT 521 5 DAYS

SECURITY MANAGEMENT

DO YOU KNOW HOW TO:

VULNERABILITY MANAGEMENT

☑ **Build a vulnerability management program**
- Asset Management
- Vulnerability Management Governance Model
- Vulnerability scanning architecture and design

☑ **Analyze and prioritize vulnerabilities**
- CVSS severity scores and ratings
- Leverage asset context
- Root cause analysis
- STIX, TAXII, STAXX

☑ **Report and communicate vulnerability data**
- Metrics Hierarchy
- Define reporting frequency

☑ **Treat and remediate vulnerabilities to manage risk**
- PIACT Process
- Automated patch management
- Hardening and configuration guidance and templates

☑ **Build relationships and processes to make vulnerability management fun**
- Relationship Map
- Define incentives, set goals, hold challenges, reward effort

MGT 516 5 DAYS

SECURITY CONTROLS

☑ **Implement and automate critical security controls**
- Minimum controls baselines and sensors
- PowerShell commands and scripting
- Windows Management Instrumentation (WMI)
- IPost reporting and data feeds
- Security Content Automation Protocol (SCAP)

☑ **Measure effectiveness of security controls**
- Measures and metrics for the CIS controls
- CIS-CAT to audit configurations
- Root cause analysis
- Vulnerability scanning
- Red Team exercises & penetration testing

☑ **Manage projects, programs, and initiatives to successful completion**
- Project Management Hierarchy
- Project Management Information System (PMIS)
- Project Priority Triangle
- Work Breakdown Structure
- Deming's Plan-Do-Check-Act (PDCA) cycle
- RACI Matrix
- Thomas-Kilmann Conflict Model
- Risk Breakdown Structure (RBS)
- Decision Tree Analysis

☑ **Build dashboards for security and compliance**
- Using spreadsheets as data sources and as visualization tools
- Configuring Graphite and loading data
- Adding Grafana data sources and building dashboard
- Building tactical reports directly from acquired data using pivot tables and graphs

☑ **Plan and execute effective audits**
- Scoping to cover highest risk areas
- Effective audit reports
- Approved baseline configurations
- Scripting audit tasks

SEC 566 5 DAYS

SECURITY OPERATIONS

☑ **Build a Security Operations Center (SOC)**
- SOC Functional Model
- Collect, Detect, Triage, Investigate, Respond

☑ **Lead incident response planning and execution**
- RE&CT Framework
- Hardening, Telemetry, Process, and Practice
- Plan activities

☑ **Develop analysis techniques, playbooks, and detection use cases**
- MITRE ATT&CK for use cases
- Sigma and YARA for detections
- Jupyter for data analysis and threat hunting

☑ **Create metrics and strategies for SOC improvement**
- Metrics vs. KPIs. vs. OKRs

☑ **Implement training and retention strategies to prevent burnout**
- SOC Human Capital Model

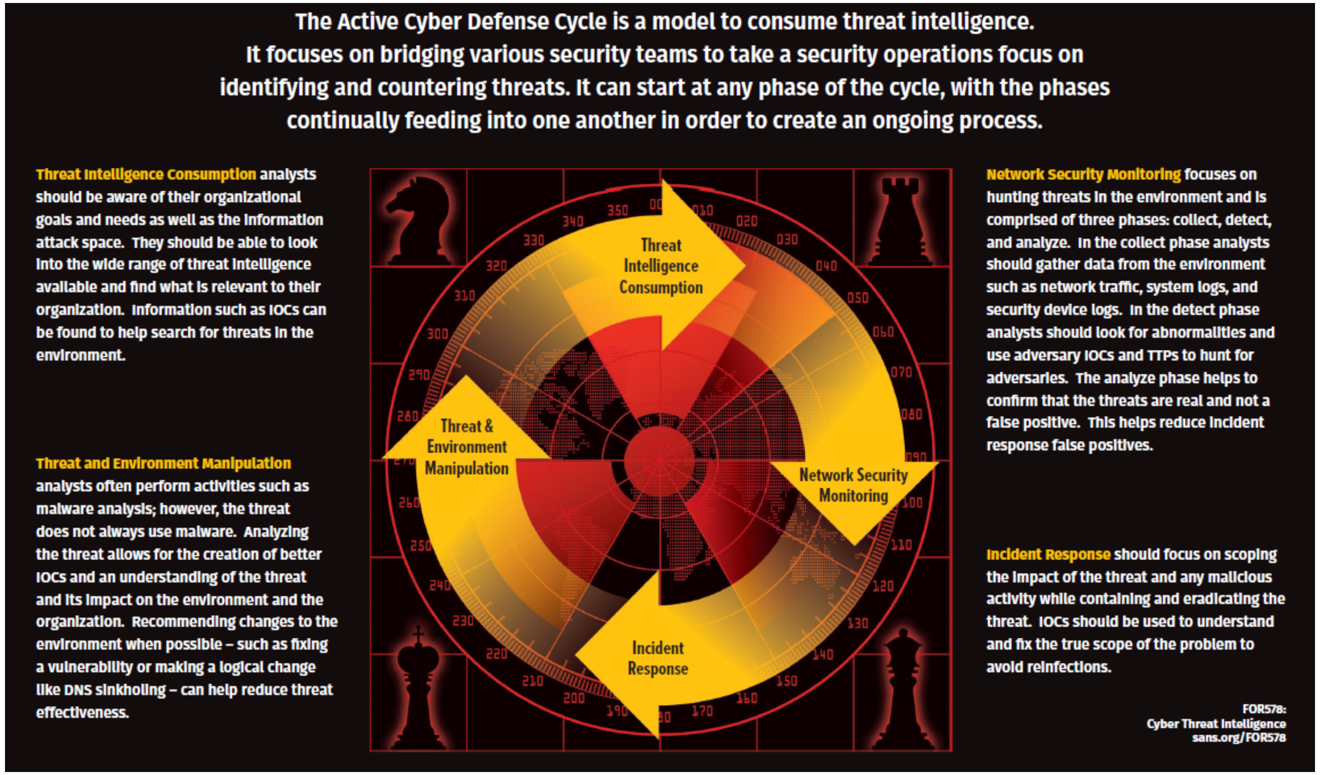
MGT 551 5 DAYS

SANS.ORG

CISOs Day to Day Life

Change of Compliance and Regulations.
Change of Technology.
Change of Threats Landscape.
Change of Circumstances (e.g. Disasters).
Change of Business Needs and Priorities.
Change of Organization.
Change of Financial Situation and Budget.
……

Active Cyber Defense Cycle



The Active Cyber Defense Cycle is a model to consume threat intelligence. It focuses on bridging various security teams to take a security operations focus on identifying and countering threats. It can start at any phase of the cycle, with the phases continually feeding into one another in order to create an ongoing process.

Threat Intelligence Consumption analysts should be aware of their organizational goals and needs as well as the information attack space. They should be able to look into the wide range of threat intelligence available and find what is relevant to their organization. Information such as IOCs can be found to help search for threats in the environment.

Threat and Environment Manipulation analysts often perform activities such as malware analysis; however, the threat does not always use malware. Analyzing the threat allows for the creation of better IOCs and an understanding of the threat and its impact on the environment and the organization. Recommending changes to the environment when possible – such as fixing a vulnerability or making a logical change like DNS sinkholing – can help reduce threat effectiveness.

Network Security Monitoring focuses on hunting threats in the environment and is comprised of three phases: collect, detect, and analyze. In the collect phase analysts should gather data from the environment such as network traffic, system logs, and security device logs. In the detect phase analysts should look for abnormalities and use adversary IOCs and TTPs to hunt for adversaries. The analyze phase helps to confirm that the threats are real and not a false positive. This helps reduce incident response false positives.

Incident Response should focus on scoping the impact of the threat and any malicious activity while containing and eradicating the threat. IOCs should be used to understand and fix the true scope of the problem to avoid reinfections.

Threat Intelligence Consumption
Network Security Monitoring
Incident Response
Threat & Environment Manipulation

FOR578:
Cyber Threat Intelligence
sans.org/FOR578

Fruit for Thought …

- Challenging four steps in normal circumstances.
- Imagine if the teams for CSIRT, SOC, SecurityEngineers, Network Teams, etc are split into more than one service providers.

The Ultimate Goal is

Winning the Cyber War:
Good vs Evil

Knowing we will have to lose some battles on the way.

The History of the Cyber World.

The First Times 1970s, 1980s

Internet for All 1990s

Internet Everywhere 2000-2010

One Global Connection

2010-Today

The First Times

1970 Arpanet

1971 Creeper and Reaper

1972 First Email, “@”

1974 TCP, Telnet, and Altair

1977 The Trinity PCs

1979 Mitnick Attack

1980 First Outage

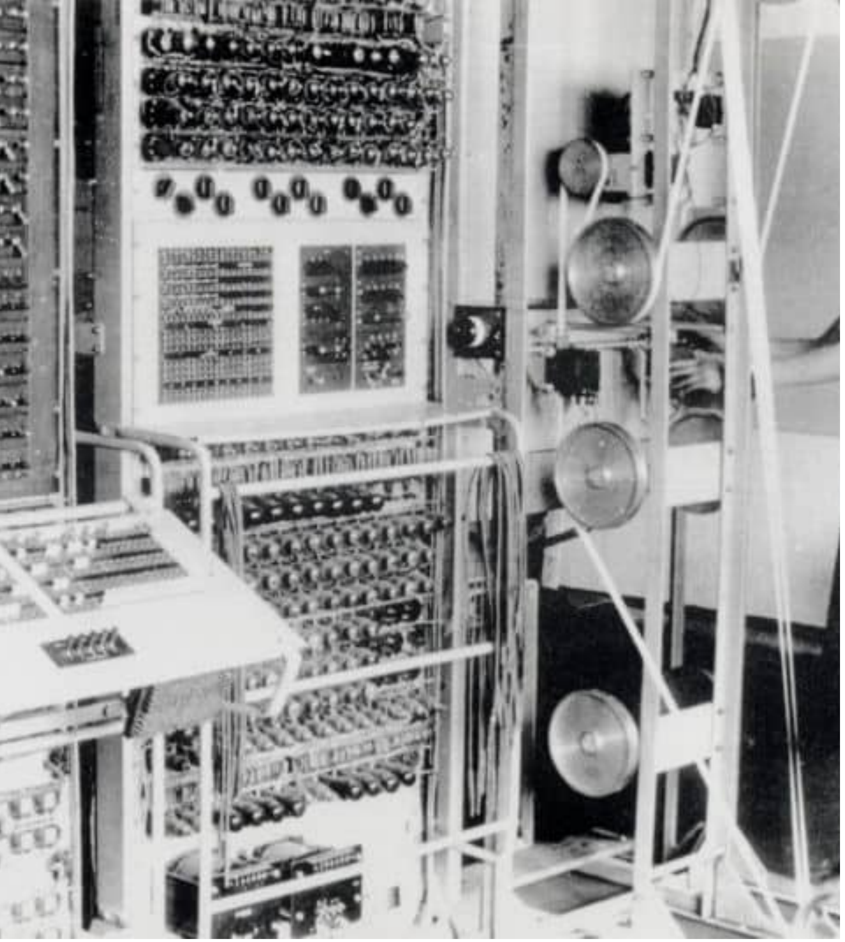
1981 IBM

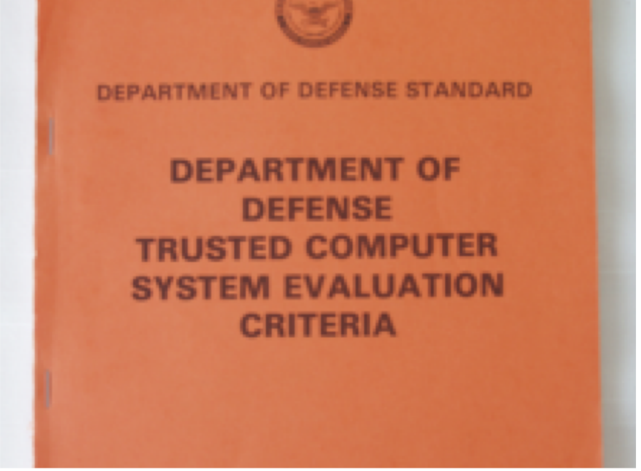
1982-1983 TCP/IP and DNS

1983 Poulsen Attack

1985 The Orange Book

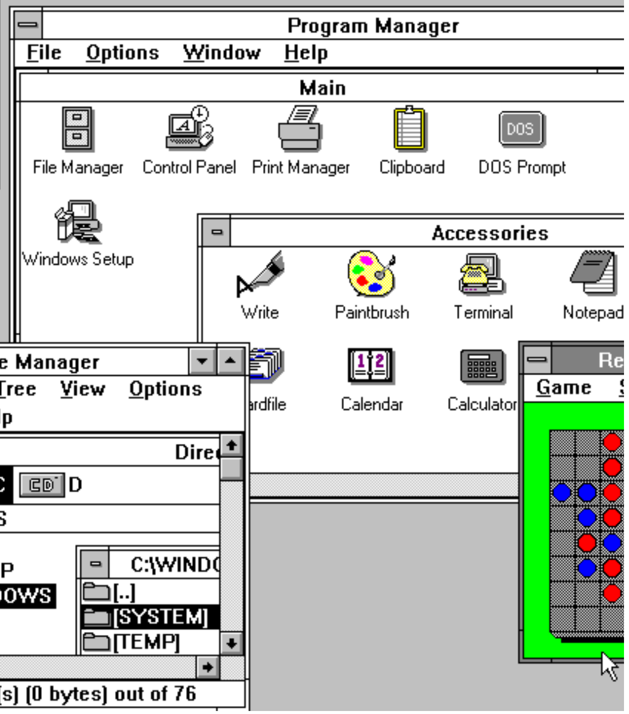
1989 First Ransomware

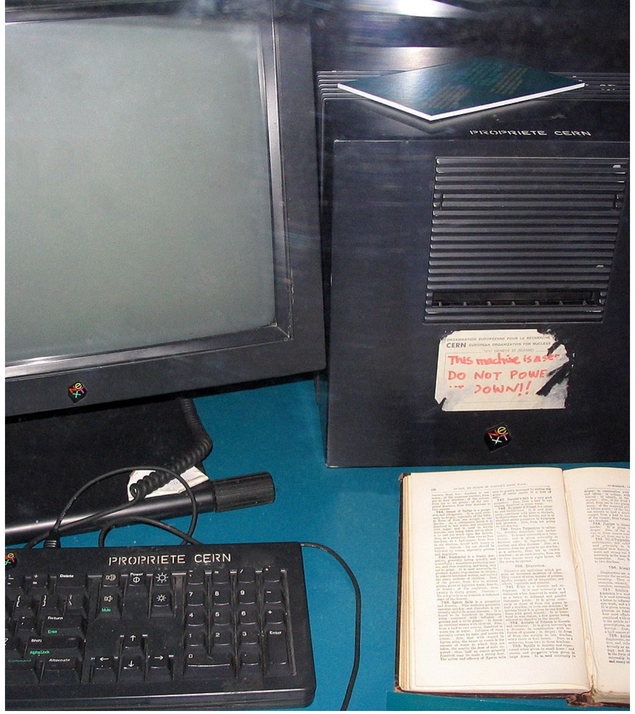




DEPARTMENT OF DEFENSE STANDARD

DEPARTMENT OF
DEFENSE
TRUSTED COMPUTER
SYSTEM EVALUATION
CRITERIA





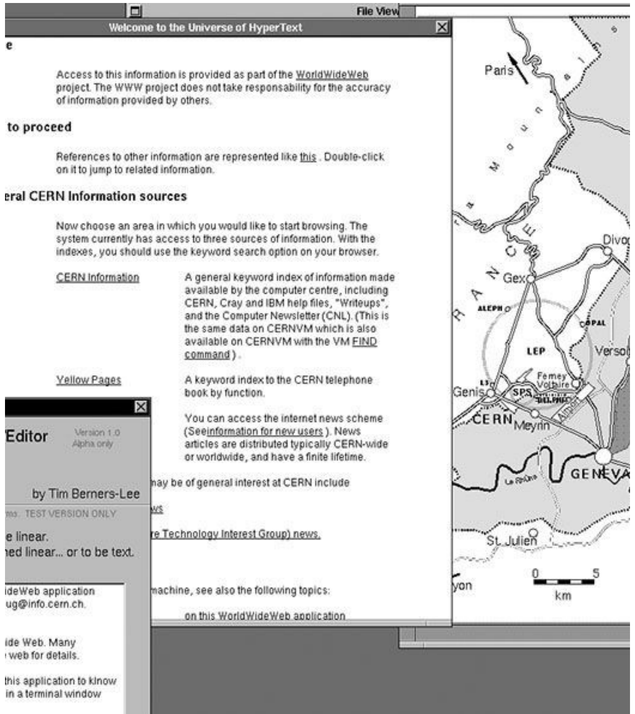
Connect to My Connection

Action

Dialing attempt 1 of 5.

Status

Dialing...



e

Access to this information is provided as part of the WorldWideWeb project. The WWW project does not take responsability for the accuracy of information provided by others.

to proceed

References to other information are represented like this . Double-click on it to jump to related information.

eral CERN Information sources

Now choose an area in which you would like to start browsing. The system currently has access to three sources of information. With the indexes, you should use the keyword search option on your browser.

CERN Information	A general keyword index of information made available by the computer centre, including CERN, Cray and IBM help files, "Writeups", and the Computer Newsletter (CNL). (This is the same data on CERNVM which is also available on CERNVM with the VM FIND command) .
Yellow Pages	A keyword index to the CERN telephone book by function.
	You can access the internet news scheme (Seeinformation for new users). News articles are distributed typically CERN-wide or worldwide, and have a finite lifetime.

nay be of general interest at CERN include

ws

re Technology Interest Group) news.

nachine, see also the following topics:

on this WorldWideWeb application

Editor Version 1.0 Alpha only

by Tim Berners-Lee

TEST VERSION ONLY

e linear.
ned linear... or to be text.

ideWeb application
ug@info.cern.ch.

ide Web. Many
web for details.

this application to know
in a terminal window

Internet for All

- Birth of World Wide Web.
- Better Hardware and Smaller Chips.
- Better Operating Systems and Software
- Affordable Equipment for the average middle class families.

Internet Everywhere

- Better Hardware Battery Life, Size, Lightness, etc.
- Better Connectivity and Wireless Connection
- The advancement of 3G and 4G network
- Smart Phones, Tablets and Laptops for every individual in the household
- The Cloud services (AWS, AZURE, GOOGLE)
- Expiring of Floppy, CD, DVD, Tapes, USB and moving more and more online
- Social Media was on the rise.

WEB 2.0
INTERNET
COMMUNITIES
CREATIVITY
BLOGS
WWW
PRIVACY
NETWORK
WIKIS
VIDEO SHARING
INTERACTIVITY
SOCIAL
PARTICIPATION

One Global Connection

theiotmagazine.com

- Cloud Computing
- IoT Advancing
- Edge Computing
- Artificial Intelligence taking a turn
- Full Connectivity

When did the Dark Web as a concept get created?

Option 1: The first times

Option 2: Internet for all

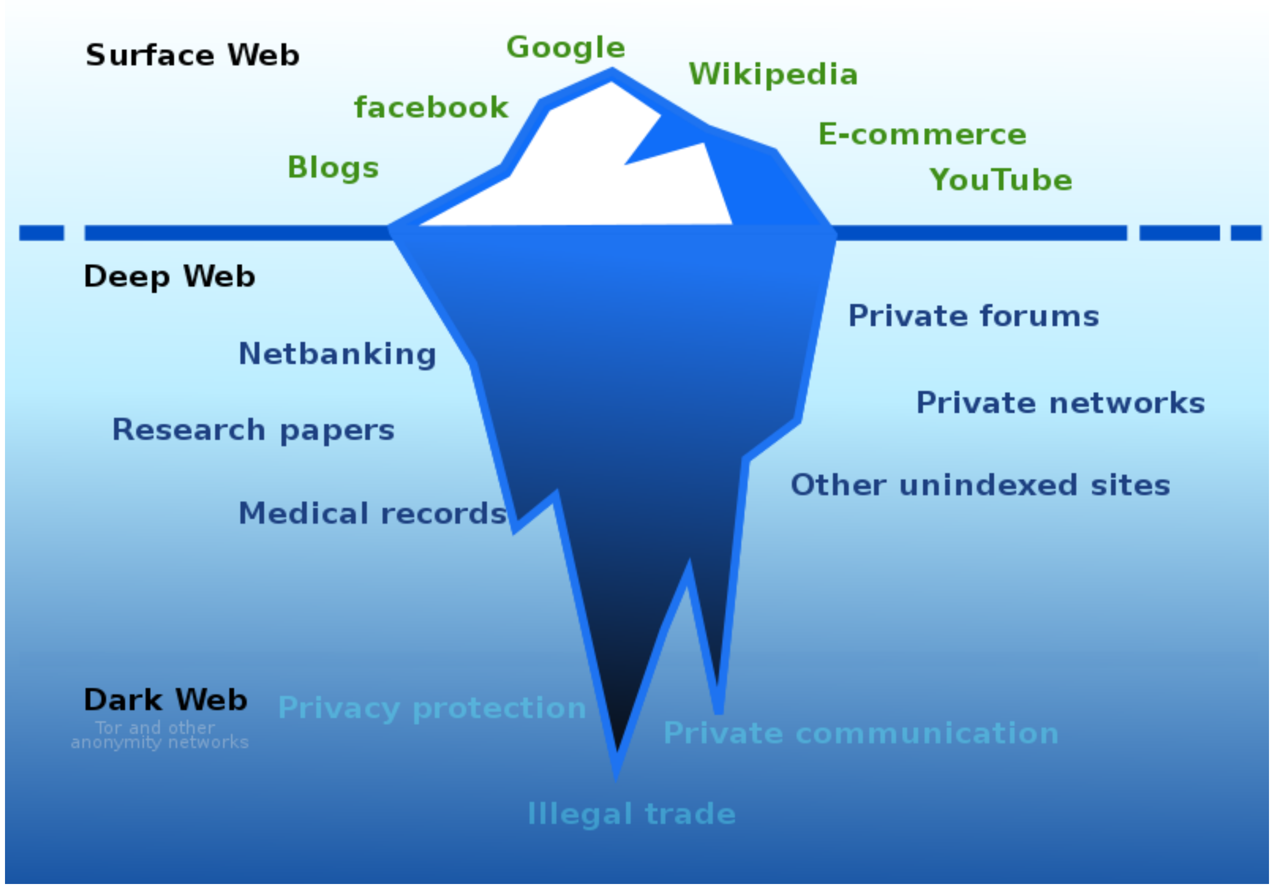
Option 3: Internet Everywhere

Option 4: We are still waiting for it

Demystifying the Dark Web

SANS.ORG The Dark Web consists of systems on the Internet designed for communicating or sharing information securely and anonymously. The Dark Web is collections of different systems and networks managed by different people used for a variety of purposes. These systems are still connected to and are part of the Internet; however, you will generally not find them using your normal search engines. You often also need special software on your computer to find or access them.

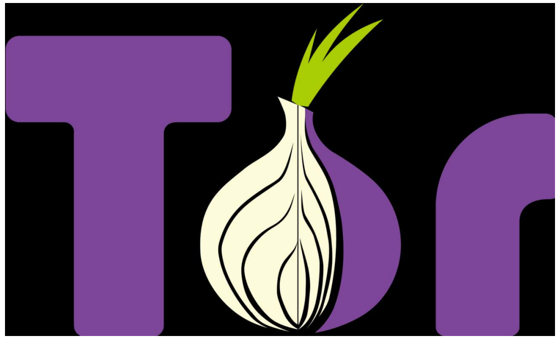
Wikipedia The dark web is the World Wide Web content that exists on darknets: overlay networks that use the Internet but require specific software, configurations, or authorization to access. Through the dark web, private computer networks can communicate and conduct business anonymously without divulging identifying information, such as a user's location. The dark web forms a small part of the deep web, the part of the Web not indexed by web search engines, although sometimes the term deep web is mistakenly used to refer specifically to the dark web. The darknets which constitute the dark web include small, friend-to-friend peer-to-peer networks, as well as large, popular networks such as Tor, Freenet, I2P, and Riffle software operated by public organizations and individuals.



Wikimedia

Dark Web History.

- 1972 Stanford-MIT Marijuana Transaction
- 1980s Data Havens
- 1990s US Naval Research Lab (onion routing)
- 2000 Freenet, sealand
- 2002 Release of Tor
- 2009 Bitcoin
- 2010 Arabian Spring
- 2011-2013 Silk Road



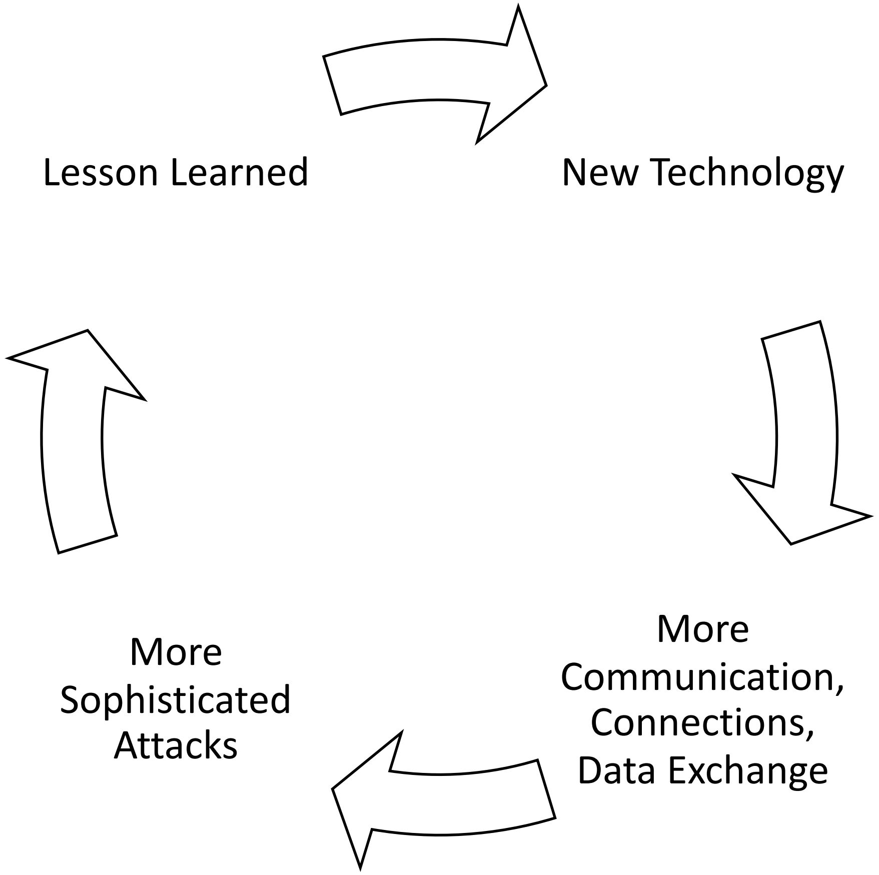
Good or Evil

- Edward Snowden: “Encryption; the defense against the dark arts for the digital realm". *NSA Leaks 2013*
- Julian Assange: "It turns out that it's easier in this universe to encrypt information, much easier than it is to decrypt it if you're someone watching from the outside... the universe fundamentally favours privacy.” *wikileaks 2006*

Tor Stats TrueList 2022

- Over 2 million users access the Tor platform daily.
- Visits to the dark web account for only 1.5% of the entire Tor traffic.
- Only 45% of websites on the dark web host illicit activities.
- Tor hosts over 65,000 unique URLs with the .onion extension.
- Of 200 domains marked as illegal on Tor, 75% are marketplaces.
- Bitcoin transactions on the dark web were on track to reach $1 billion in 2019.

Winning the Cyber War: Good vs Evil

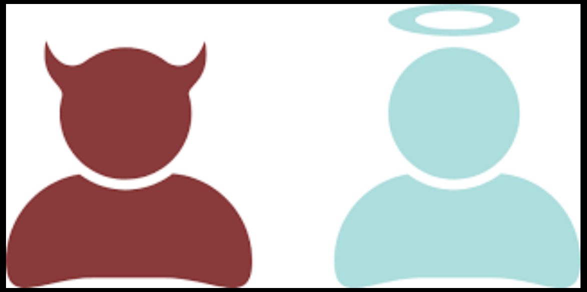

Lesson Learned

New Technology

More Communication, Connections, Data Exchange

More Sophisticated Attacks

- Stay Informed
- Hire Excellent Staff/Providers
- Ensure a Strong Network (Share and Care)
- Engage in the Business Continuously
- Offense Guides Defence



Every war in history has an end

Except the war between Evil and Good

Nevertheless, Good can balance out Evil