

Will Cyberspace Ever Be Secure?

Presentation and Discussion
for the Osher Lifelong Learning Institute (OLLI)
at American University

Dr. Eric J. Novotny
School of International Service

What is cyberspace?
What does it mean to be secure?





US-China Meeting Anchorage, Alaska 19 March 2021

Secretary Blinken: “We’ll also discuss our deep concerns with actions by China, including in Xinjiang, Hong Kong, Taiwan, cyberattacks on the United States and economic coercion toward our allies. Each of these actions threaten the rules-based order that maintains global stability. That's why they're not merely internal matters and why we feel an obligation to raise these issues here today.”



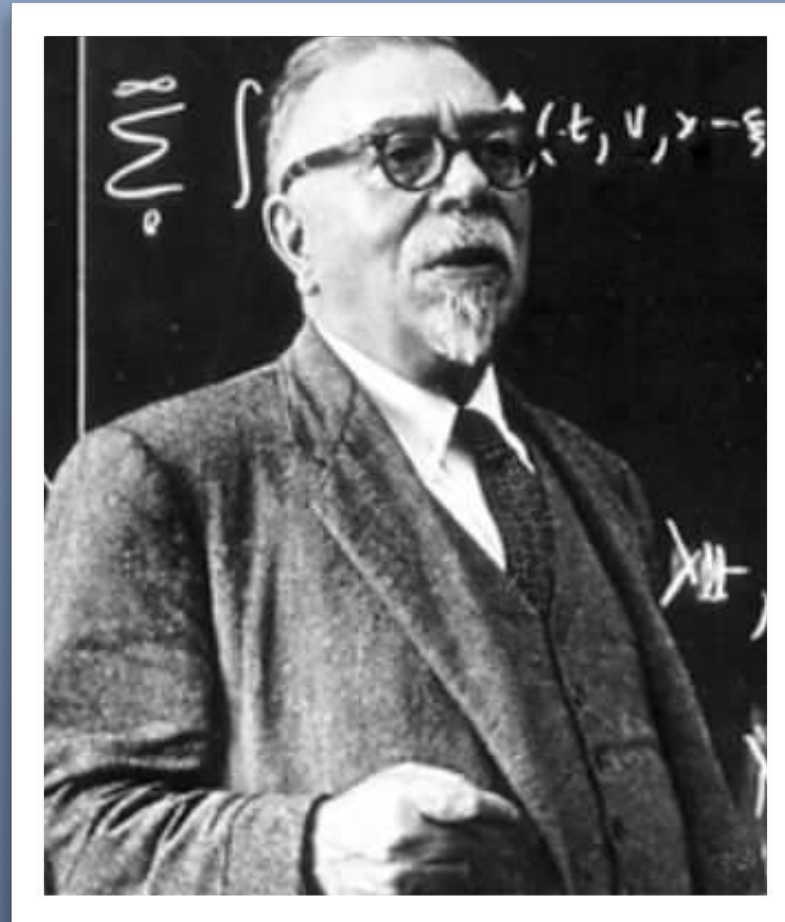
Director Yang Jiechi: “On cyberattacks, let me say that whether it's the ability to launch cyberattacks or the technologies that could be deployed, the United States is the champion in this regard. You can't blame this problem on somebody else.”



Derived from “Cybernetics”
or
the process of
communication as defined by
information theory

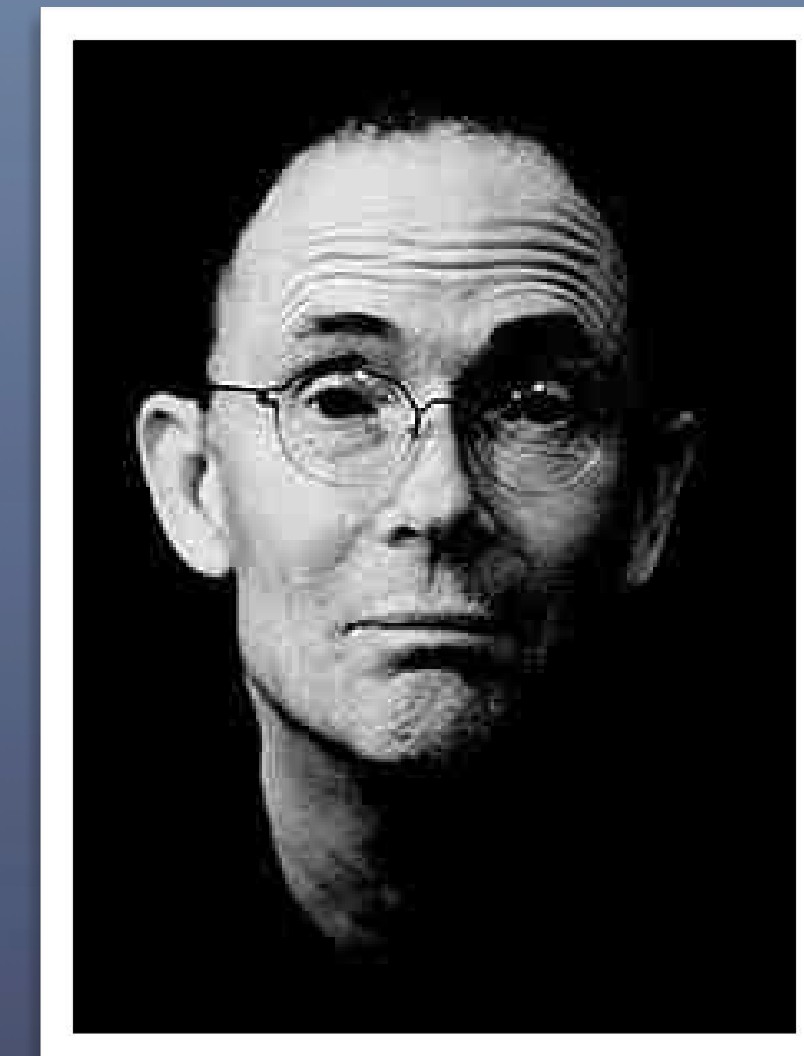
Κυβερνήτης, "KUBERNETES" GREEK WORD FOR "STEERSMAN"

André-Marie Ampère (1775-1836) used the word cybernetics to denote "the study of ways of governing."



Mathematical foundations of control theory laid down by Norbert Wiener in *Cybernetics* (1948) and in *The Human Use of Human Beings* (1950)

Linked to "space" to become "cyberspace" by William Gibson in *Burning Chrome* (1982)



“Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding...”

— William Gibson, *Neuromancer*

Terms, definitions, and names





DEFINITION

Cyberspace—The notional environment in which communication over computer-based networks occurs

or

The realm of electronic information

A NOTE ON NAMES AND NOMENCLATURE

TITAN RAIN
ROCKET KITTEN
LAZARUS GROUP
SHADOW BROKERS
APT-28
NOTPETYA
STUXNET
HEARTBLEED
WANNA CRY
FANCY BEAR
MELTDOWN
MIRAI BOTNET

In the literature and in the media, you will encounter many different names for certain threat actors, pieces of malware, techniques, vulnerabilities, incidents, and so forth

Please keep in mind that there are almost no standards or conventions for such names in the cyber security field except by customary use and repetition



DEFINITION

Threat—A potential malicious action taken against an information system or network

Threat Actor—An individual or group organized to carry out threats— sometimes called an “intrusion set”

Threat Effect—Compromise or damage to confidentiality, integrity or availability of information

Vulnerability—A weakness or hazard that may be used by a threat actor

Tactics, Techniques and Procedures—**TTPs**—The technical and operational methods employed by a threat actor

Indicators of Compromise—**IOCs**—Evidence that a data breach or other loss has taken place or that a threat actor has successfully penetrated a network

Computer Network Intrusion—**CNI**—Access to a network by a threat actor or unauthorized user

Computer Network Exploitation—**CNE**—After a CNI has taken place, the actions by a threat actor to exfiltrate, alter, or destroy information

Computer Network Attack—**CNA**—After a CNE has taken place, the actions by a threat actor to attempt physical damage or loss of life

Cyber Incident—Generic term for any attempted or successful action by a threat actor

Cyber Campaign—An organized, persistent effort by a threat actor against a specific target

THE "CYBER CANON"



<https://cybercanon.paloaltonetworks.com/#allwinners>

PODCASTS, BLOGS, AND NEWSLETTERS

Daily “Push” Newsletters:

CyberWire Daily

CyberScoop

The Hill (Cyber)

The Hacker News

Lawfare

War on the Rocks

Fifth Domain

Recorded Future Cyber Daily

Washington Post Cyber 202

Best Weekly or Monthly Newsletters:

Cryptogram (Bruce Schneier)

UC-Berkeley: Center for Long-Term Cyber Security

securityroundtable.org

Krebs on Security

PodCasts:

CyberWire Daily

Hacking Humans

Recorded Future

Darknet Diaries



COMPONENTS OF THE CYBER DOMAIN

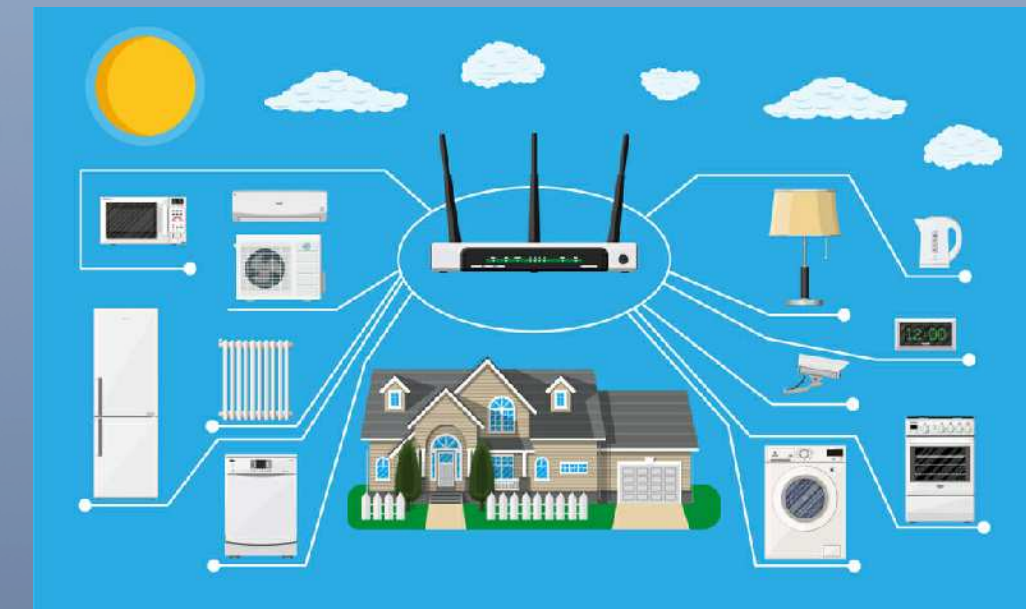
Physical Layer

Includes the telecommunication infrastructure like cables, satellites and switches; includes all devices such as servers, routers, end-point devices



Logical Layer

Includes all of the software to run networks—protocols, technical processing tasks (OSI stack), application programs and operating systems



Data Layer

Any information or information asset produced, collected, stored or processed through a network or database

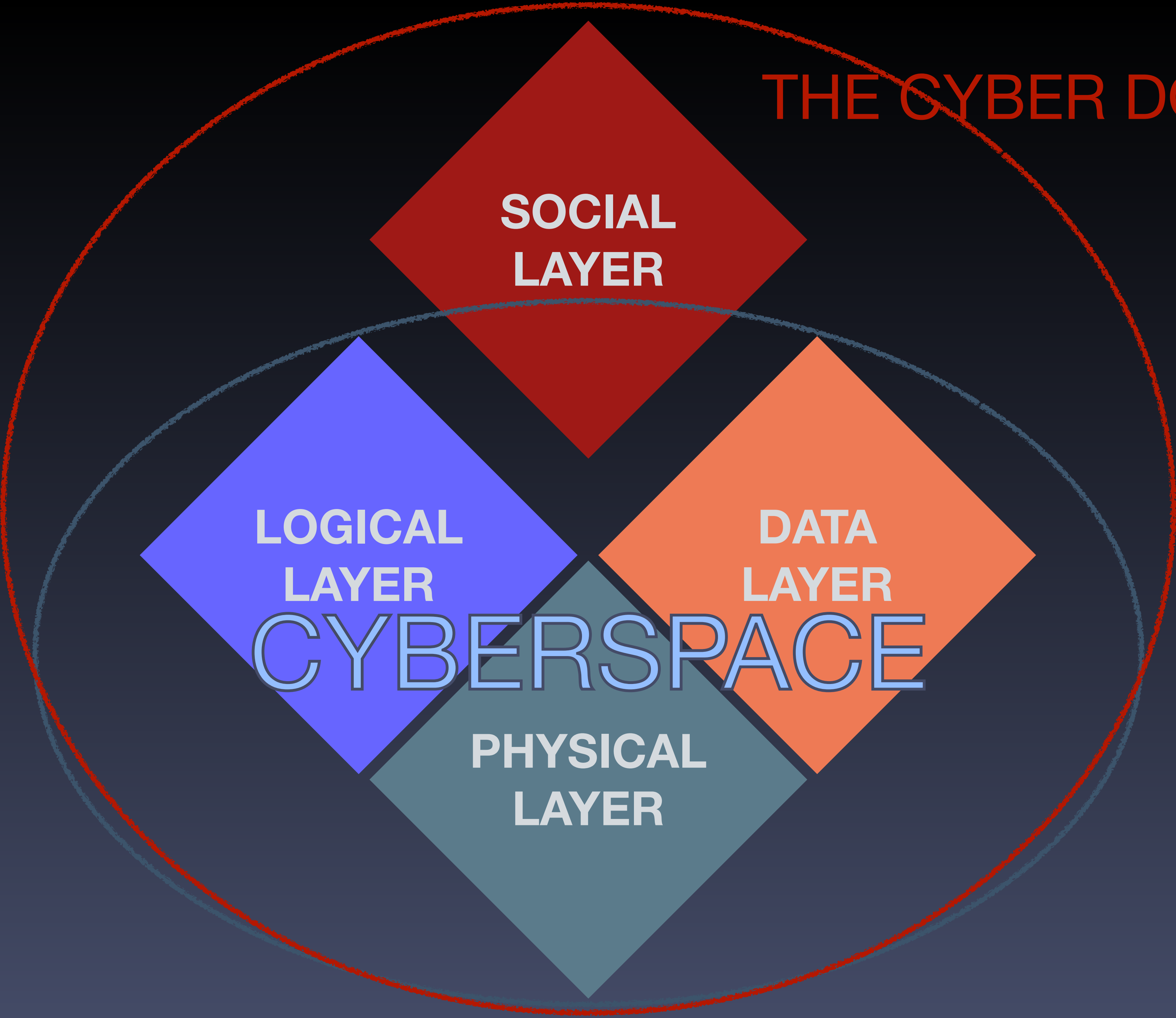


Social Layer

All of the human interactions or human-to-machine interactions that occur through information appliances, devices, or networks



THE CYBER DOMAIN



SOCIAL
LAYER

LOGICAL
LAYER

DATA
LAYER

PHYSICAL
LAYER

CYBERSPACE

ATTRIBUTES OF THE CYBER DOMAIN

Ambiguous

It is logical or virtual rather than real even though it has physical representations



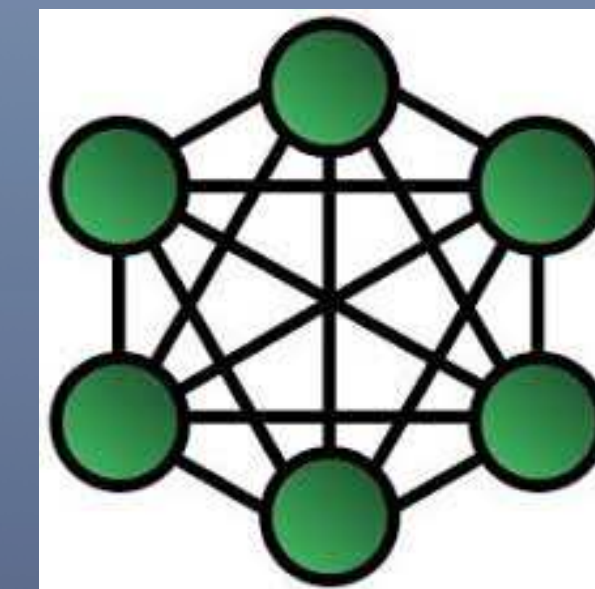
Distance Invariant

To human perception, locations either near or far make little or no difference



Interactive

Users, groups, entities of any kind are in theory all interconnected—Communication is “mesh-like” or a many-to-many network or networks



Ubiquitous

Cyberspace is expansive because can touch any process or decision that is computable—the stock of stored information is growing and does not go away



What is Cyber Security?



THREE INFORMATION "STATES"

Information at Rest

Databases, records, password vaults, etc., that are residing on a server or other device and are in turn accessible by authorized and trusted users or open to the public, such as a website



Information in Motion

When information of any kind such as email records, chat records, account information, contact lists, etc., are on a device that is transportable—smartphones, laptops, flash drives



Information in Transit

Any information or information asset sent or received electronically through a network, such as through a wifi router



THREAT EFFECTS

Confidentiality

The quality of shared information remaining within an authorized, trusted domain. Violations of confidentiality include data breaches, theft of intellectual property, or other forms of espionage



Integrity

Threats to integrity are those which alter information in some way to the disadvantage of the owner, such as financial fraud or disinformation through altered records



Availability

When an information asset or network is not available to a person or industrial process when it is needed. Examples include disabling an industrial control system, such as an electric power plant to electrical grid



COMPONENTS OF CYBER SECURITY

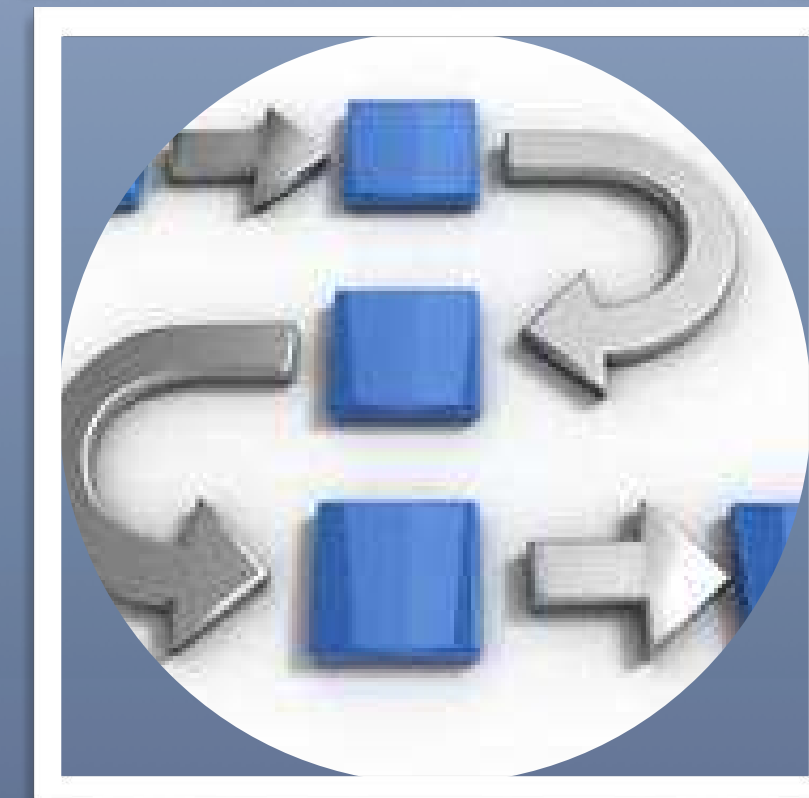
People

Many cyber defenses depend on the education, training and vigilance of an organizations' people; many vulnerabilities can also stem from person-to-person relationships; offensive cyber operations, including criminal activities also originate with persons or in groups



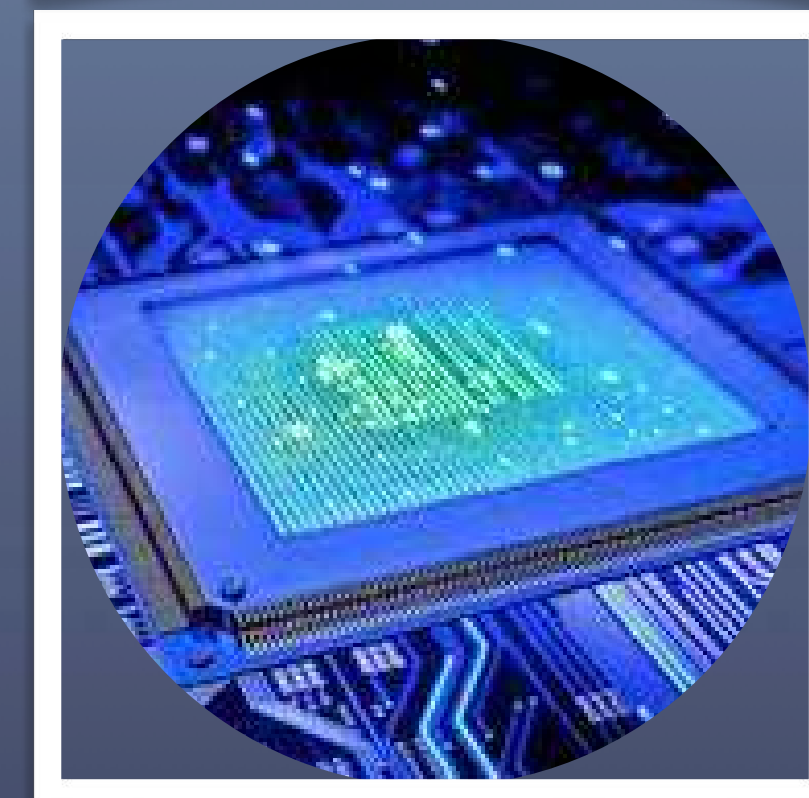
Processes

Administrative rules, policies, legal compliance requirements and organizational relationships, such as in a supply chain, affect the vulnerabilities present in an information system or network



Technology

Because cyberspace is inherently a technological phenomenon, many security solutions have a strong technical component; likewise, threat actors can exploit technical vulnerabilities in networks to intrude, exploit, deny degrade or destroy an information asset





DEFINITION

CYBER SECURITY

The use of:

People, Processes, and Technology

to protect the

Confidentiality, Integrity, or Availability

of assets in cyberspace that are

in Motion, at Rest or in Transit

THE CYBER DOMAIN POSES SERIOUS CHALLENGES


Attackers have the advantage

Trying to understand all the intricacies of securing information assets is not so simple as it might seem

All cyber security methods, procedures, or policies are “dual use”

The need for cyber security measures is usually not recognized until it is too late and is sometimes regarded as an impediment to efficiency or convenience—there is no easy way to balance ends and means

We have not learned lessons from the past



*SolarWinds:
A Case Study in Cyber Network Intrusion*

WHAT HAPPENED

Commercial cyber security company FireEye discloses publicly that its “red team” active defense and threat detection toolkits were exfiltrated by an unknown threat actor and used against its customers

FireEye traces the intrusion to an IT network and infrastructure platform called Orion, from a supplier called SolarWinds

FireEye was penetrated after a sophisticated set of malware was smuggled in a software update from SolarWinds—one malware tool was then able to spoof registration of a new laptop on the FireEye network and then escalate privileges, import further malware tools, and move laterally inside FireEye impersonating a legitimate user

Once the malware signatures are identified, it appears that the Orion update was distributed to 18,000 SolarWinds customers (SolarWinds has 300,000 customers), including at least 10 federal government agencies and 450 of the Fortune 500

Further forensic investigations have uncovered the presence of this intrusion going back to 2019

Note: This intrusion is an evolving situation and information about it may become superseded at any time

SOLARSTORM TIMELINE



WHAT WE KNOW AND DO NOT KNOW

No authoritative information has been released about how the malicious code entered the Orion library that is used to update its software remotely with SolarWinds customers

No government agency has disclosed what it knew, what it detected, or failed to detect—only advisories after the FireEye blog post

The threat actor embedded backdoor code into a legitimate SolarWinds library with the file name `SolarWinds.Orion.Core.BusinessLayer.dll` and then these “trusted” updates are sent to Orion’s users

While updating Orion, the embedded malware loads (and hides) before the legitimate code executes, so the user is misled into believing that no malicious activity has occurred and that update is working properly, using the victims’ own digital certificates to establish false trust

The malicious file then contacts a remote command and control infrastructure to prepare second-stage payloads, move laterally in the network, and either exfiltrate, change or prepare to destroy data

ALLEGATIONS OF INSIDER TRADING

SolarWinds is being investigated by federal and state financial regulatory authorities for potential insider trading

Representatives from private equity investors Silver Lake and Thoma Bravo made up a majority of SolarWinds' 11-member board, and owned more than 75 percent of SolarWinds' outstanding shares in April 2020, according to a U.S. Securities & Exchange Commission filing

These investors sold more than 13 million share of SolarWinds stock at \$21.97 per share on December 7th, 48 hours before the IT infrastructure management firm announced a new CEO

On December 11th, FireEye notifies SolarWinds and the US government and goes public with the initial details

The US National Security Council calls an emergency meeting on December 12th

As of January 15th, SWI was selling at \$15.82, a decrease of 28 percent

SWI TRADING ON THE NYSE

Switch Quote

SWI U.S.: NYSE

SolarWinds Corp.

AFTER HOURS

\$15.82

▼ -0.19 -1.19%

After Hours Volume: 64.4K

Last Updated: Jan 15, 2021 7:54 p.m. EST
- Delayed quote

CLOSE	CHG	CHG %
\$16.01	0.79	5.19%

VOLUME: 5.07M

65 DAY AVG: 1.83M

277% VS AVG

Join TD Ameritrade.

ADD TO WATCHLIST

CREATE SWI ALERT



15.27 DAY RANGE 16.26 11.50 52 WEEK RANGE 24.34

WHAT THIS INCIDENT MEANS

Perpetrated by a persistent, pre-meditated, well-resourced, focused threat actor that has achieved long duration intrusions on many networks

Such a method of penetrating many organizations in this manner—a software update—could be nearly impossible to either prevent or detect, especially for a federal agency like the NSA, CISA or US Cyber Command

Possible that this threat actor penetrated many organizations but discovered they could not exploit them all, did not want to exploit them all, had their tools go dormant to be activated at a later time, or used the exploit against only a few desirable targets

Recovery and remediation will be difficult, lengthy, and expensive

WE DO NOT LEARN FROM OUR MISTAKES

Thirty-seven years ago, Kenneth Thompson in his Turing Award lecture demonstrated how easily a developer could add malicious code to a software program that was difficult to detect by inserting a “bug” in a few lines of code:

“The moral is obvious. You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me.) No amount of source-level verification or scrutiny will protect you from using untrusted code.”

—“Reflections on Trusting Trust,” *Communications of the ACM*, 27 (August 1984):763.

SUPPLY CHAIN INTRUSIONS

September 2011 — Digitnotar—A certificate authority based in the Netherlands is compromised resulting in issuance of large numbers of fraudulent certificates, used to penetrate other systems

November 2013—OPM contractors, USIS and KeyPoint, are used to penetrate OPM's security clearance and fingerprint records of over 20 million people—attributed to the Chinese Cyber Army

September 2015 — XcodeGhost: A “back door” into Apple's Xcode software (used to build iOS and macOS applications), which injected additional code into iOS apps. Discovered by a Chinese developer at Alibaba and reportedly infected over 3,000 apps

March 2016 — KeRanger: A popular free BitTorrent app, Transmission, had its source code compromised that permitted a threat actor to employ ransomware extortion against users

June 2017 — NotPetya—Threat actor infected a tax and accounting app of a Ukrainian software company and smuggled ransomware and destructive elements into customers using the software, ultimately causing a worldwide disruption that cost billions of dollars—Origin was an NSA hacking tool, EternalBlue allegedly repurposed by the Russian GRU

September 2017 — CCleaner: App used to remove unwanted and unnecessary Windows files included a version with malware designed to exfiltrate information, affecting over 2 million PCs—A second compromise in 2019 although not proven that the same operators from 2017 were responsible

In all these cases, rather than targeting an organization directly through phishing or exploitation of vulnerabilities, the threat actor chose to compromise developers in the software supply chain, which vastly amplifies the number of potential targets

HOW DO WE KNOW IT WAS THE RUSSIANS?

We do not—at this point there is no definitive attribution

The (former) Secretary of State identified a Russian source in an interview on December 18, 2020

Other unnamed sources in government have identified a Russian state actor in media reports

Recorded Future performed a detailed analysis of three known Russian threat actors and found some overlap between SolarStorm and these groups—also discovered “Nine techniques are novel and not seen in...known previous incidents.” [pov-2020-1230]

Many details have not emerged as victims are in the process of either collecting information, assessing the extent of the intrusion, or not disclosing specific countermeasures before vulnerabilities can be patched or threats removed

Some known malware or dual use tools have also surfaced

WHAT DO THE SIMILARITIES SUGGEST?

The malware now known as **Sunburst** was developed by the same group as another piece of very similar malware that emerged in the incident, **Kazuar**

The **Sunburst** developers adopted some ideas or code from **Kazuar**, without having a direct connection (copying or adapting the code from to the other)

The threat actors identified as **DarkHalo** or by FireEye as **UNC2452** and the group using **Kazuar**, obtained their malware from the same source

Some of the **Kazuar** developers moved to another intrusion set or group, taking their skills and code with them

The **Sunburst** developers deliberately included these blocks of code as a form of deception or false flag operation, to deflect, confuse or shift blame to another threat actor



PRINCIPLE

Controls and safeguards in cyber security are “dual use” —A tool or technique that can be used for a positive, defensive purpose, like *Cobalt Strike Beacon*, can just as easily be turned against a network for an offensive purpose

We don't learn from our mistakes —Supply chain penetration techniques have been around a long-time—but they are also very difficult to defend against

Aggressive operations beget aggressive operations —Do we really know the motives? Was this an actor emboldened, wanting to prove its capabilities, retaliating for something done *sub rosa*, or what, really?

Thank you very much!

Wishing all of you liberty and prosperity
in a
free and secure cyberspace

Dr. Eric J. Novotny directs three graduate programs in US foreign policy and national security and is the founding director of the cyber security program at the School of International Service. He is also Vice-President of the SIS Faculty. He teaches graduate-level courses in cyber threat intelligence, technical cyber security methods and risk assessments. He was formerly senior advisor for digital media and cyber security at the US Department of State. He has held senior executive positions at Lockheed Martin Corporation and at Hughes Electronics. Novotny is a consultant to both public and private sectors in the areas of cybersecurity, cyber risk assessment, secure communication and Internet freedom and holds positions on the Board of Directors of four corporations. He is a graduate of Georgetown and Oxford Universities.

novotny@american.edu