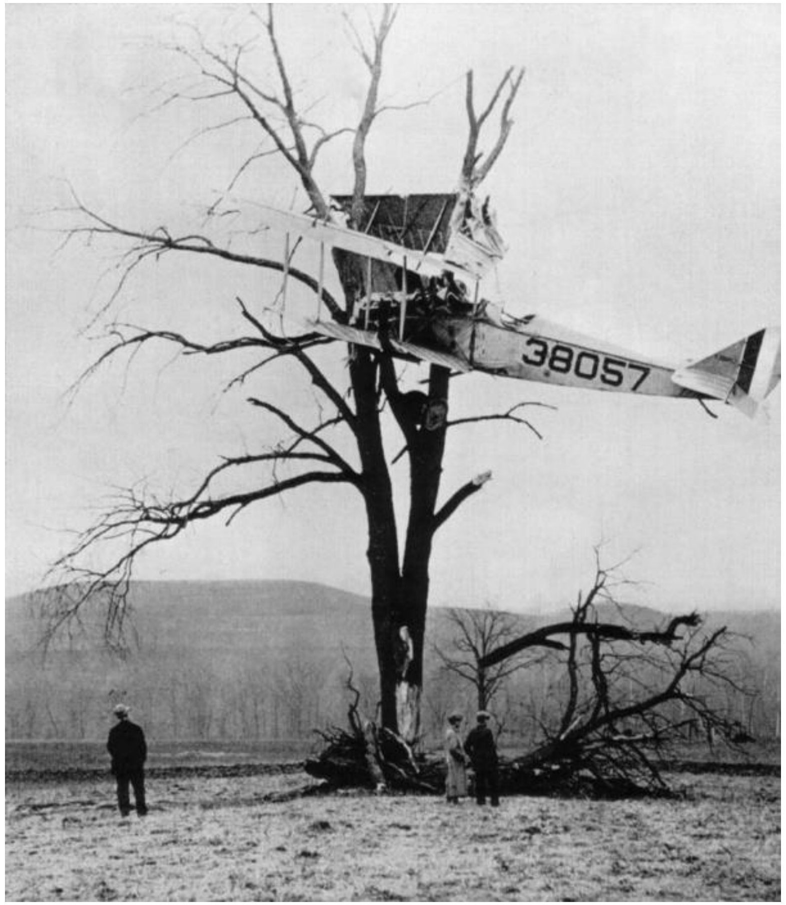


http://www.vlib.us/wwi/resources/archives/images/i050203/images/AMER%23850.jpg

Cybersecurity is inherently difficult. It is terribly unforgiving of any carelessness, incapacity, or neglect.

– With thanks to Captain A. G. Lamplugh
British Aviation Insurance Group

Legal Disclaimer

This presentation is not, and should not be considered,
legal counsel, legal advice, or legal opinion.

Only attorneys should provide legal counsel, legal advice, and legal opinions.
They can be the best friend for $800/hr.

USE THIS PRESENTATION’S INFORMATION AT YOUR OWN RISK.

All presented information represents personal opinions and current understanding.

The presenters do not assume any responsibility or liability for damages
arising from relying on or using this presentation’s information.

NO WARRANTIES ARE EXPRESSED OR IMPLIED.

Ransomware in the Era of Quantum Computing

Part 1

W. David Schwaderer
CEO/Co-founder Shape*Shift*™ Ciphers LLC
david@Shape*Shift*Ciphers.com

The Bear Joke

<u>Speed Bumps</u>

1. Amorphous System Topology
2. Amorphous Encryption
3. Amorphous Interposer Encryption

Three Takeaways

1. The Current Cybersecurity Situation is Serious

Three Takeaways

2. New Thinking and Action is Required

Three Takeaways

3. Extinction is Forever

https://upload.wikimedia.org/wikipedia/commons/0/0c/Velociraptor-by-Salvatore-Rabito-Alc%C3%B3n.jpg

The Problem

You must bat 1000.

They only have to bat greater than zero.

Is Cybersecurity Vulnerability a Solvable Problem?

In theory, yes.

But,

In theory, theory and practice are the same.
In practice, they aren’t.

- Benjamin Brewster
The Yale Literary Magazine
February 1882

Is Cybersecurity Vulnerability a Solvable Problem?

The Current Approach Appears To Be

- Piecemeal
- Fragmentary
- Reactive
- An Ad hock Improvisation Ensemble
- A Moebius, Sisyphean Journey

Is Cybersecurity Vulnerability a Solvable Problem?

The Human Element

The most important failure was one of imagination. We do not believe leaders understood the gravity of the threat.

There is no one to whom we can attribute malice or ill motives. Instead, we found systemic failures and egregious poor decision making.

Despair.com Demotivation Posters

© DESPAIR.COM
CONSULTING
IF YOU'RE NOT A PART OF THE SOLUTION,
THERE'S GOOD MONEY TO BE MADE IN PROLONGING THE PROBLEM.

https://despair.com/collections/posters

Is Cybersecurity Vulnerability a Solvable Problem?

Cybersecurity is not a Retrofit.

Solution: A Systemic Approach that embeds Cybersecurity in its Foundation

Near-term Prognosis: Poor

Is Cybersecurity Vulnerability a Solvable Problem?

High Probability Outcome

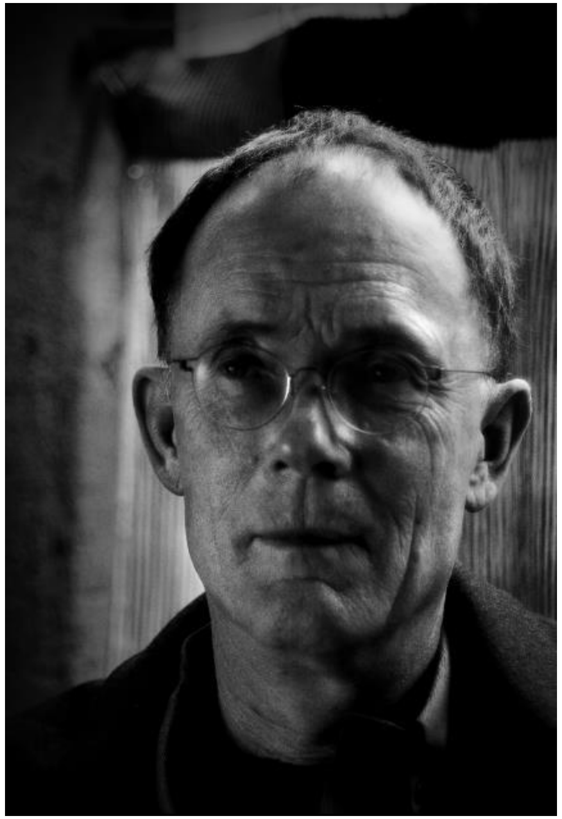
You and Your Enterprise will likely be impacted.

It’s likely a *when*, not an *if*.

It’s likely a *sooner*, rather than *later*.

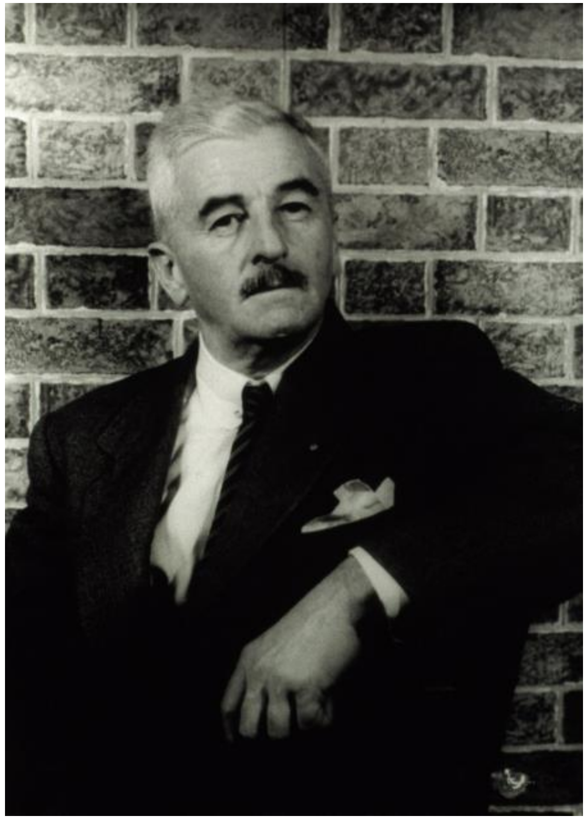
It’s Damage *Minimization*, not *Prevention*.

1970s Cybersecurity Case Study



William Gibson

The future is already here —
it’s just not very evenly distributed.



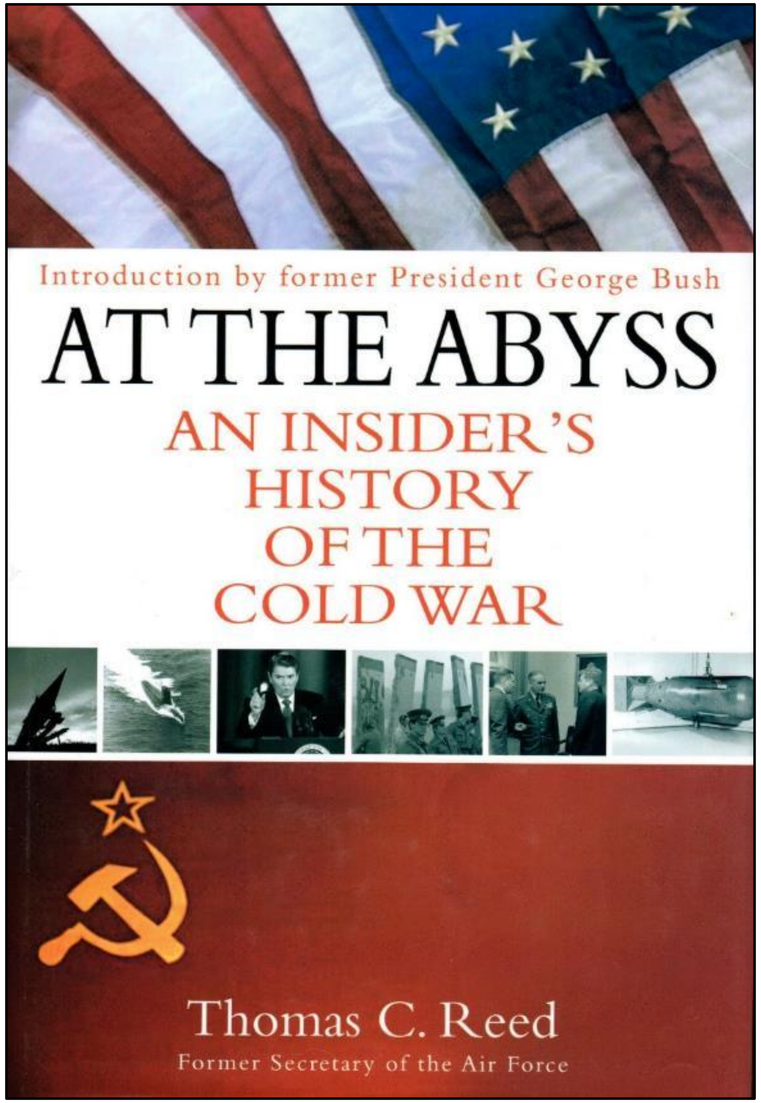
William Cuthbert Faulkner

The past is never dead.
It's not even past.

If you don't know where you are going, any road will get you there.

– Lewis Carroll

At the Abyss



Introduction by former President George Bush

AT THE ABYSS

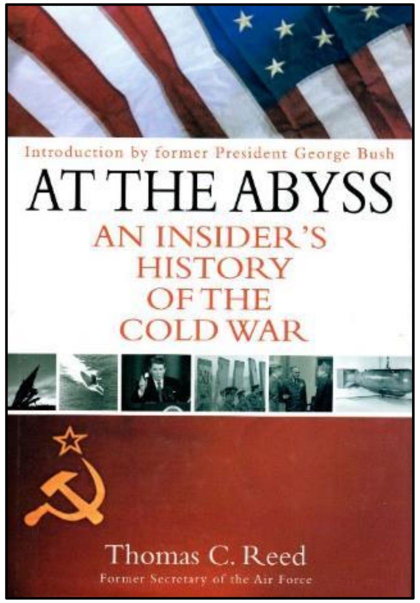
AN INSIDER'S HISTORY OF THE COLD WAR

Thomas C. Reed

Former Secretary of the Air Force

2004

At the Abyss


Introduction by former President George Bush
AT THE ABYSS
AN INSIDER'S HISTORY OF THE COLD WAR
Thomas C. Reed
Former Secretary of the Air Force

Pgs. 266-269

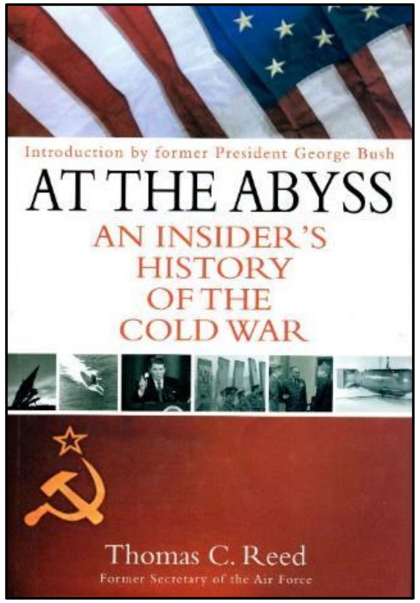
1970s Cold War

Nixon Administration: Détente

Henry Kissinger

> *… over time, trade and investment may leaven the autarkic tendency of the Soviet Union.*
>
> *… invite the gradual association of the Soviet economy with that of the world economy and thereby foster interdependence that adds an element of stability to the political relationship.*

At the Abyss



Introduction by former President George Bush

AT THE ABYSS

AN INSIDER'S HISTORY OF THE COLD WAR

Thomas C. Reed

Former Secretary of the Air Force

Pgs. 266-269

Leonid Brezhnev (1972)

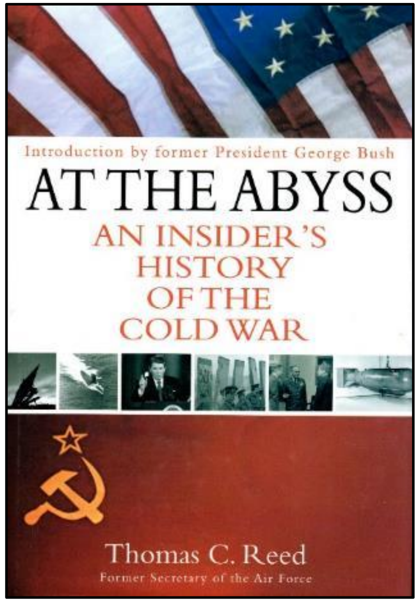
General Secretary of the Communist Party
Chairman of the Presidium of the Supreme Soviet

We communists have to string along with the capitalists for a while.

We need their credits, their agriculture, and their technology.

But we are going to continue massive military programs, and by the mid-1980s, we will be in a position to return to an aggressive foreign policy designed to gain the upper hand with the West.

At the Abyss



Introduction by former President George Bush

AT THE ABYSS

AN INSIDER'S HISTORY OF THE COLD WAR

Thomas C. Reed

Former Secretary of the Air Force

Pgs. 266-269

<u>July 19, 1981</u>

President Ronald Reagan Ottawa conversation with President François Mitterand

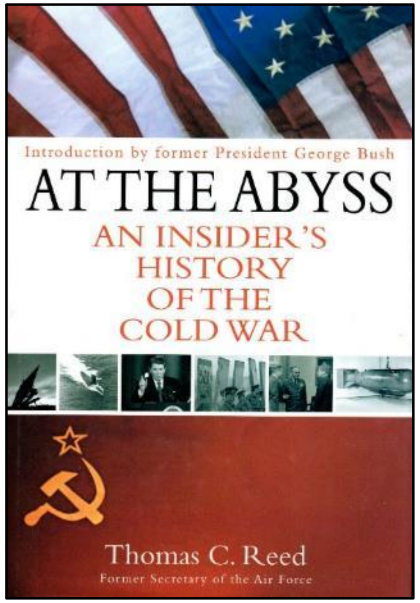
France had a deep mole in the Soviet's KGB - codename *Farewell*.

Farewell reviewed Soviet Western technology purchases/thefts by the KGB's *Line X* group

US received an *incredibly explicit Farewell* **<u>Dossier</u>** detailing penetrations of Western

- Laboratories
- Factories
- Governments

At the Abyss


Introduction by former President George Bush
AT THE ABYSS
AN INSIDER'S HISTORY OF THE COLD WAR
Thomas C. Reed
Former Secretary of the Air Force

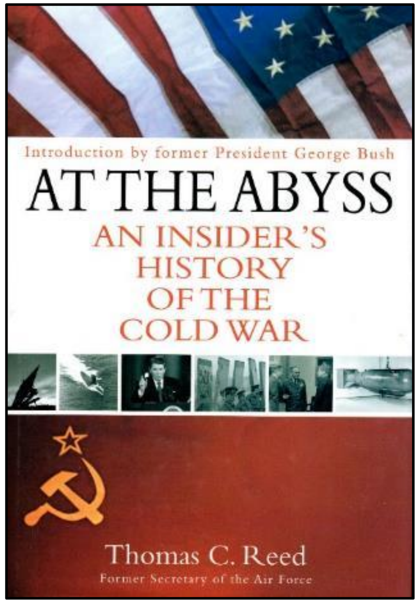
Pgs. 266-269

The *Farewell* **Dossier** proved the Soviets had been running their R&D *on the West's back* for years.

The Pentagon had been in *an arms race with itself*.

- Radars
- Computers
- Machine tools
- Semiconductors

At the Abyss

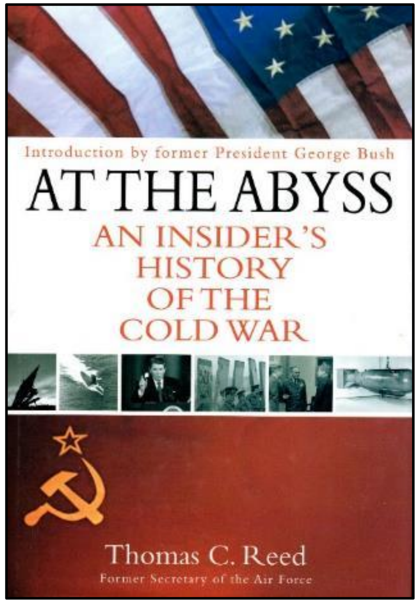

Introduction by former President George Bush
AT THE ABYSS
AN INSIDER'S HISTORY OF THE COLD WAR
Thomas C. Reed
Former Secretary of the Air Force

Pgs. 266-269

The *Farewell* **<u>Dossier</u>** Identified Western and Japanese

- Agents (Named Hundreds)
- Information Suppliers
- Parts Suppliers
- **Technology Acquisition and Theft Targets**

At the Abyss


Introduction by former President George Bush
AT THE ABYSS
AN INSIDER'S HISTORY OF THE COLD WAR
Thomas C. Reed
Former Secretary of the Air Force

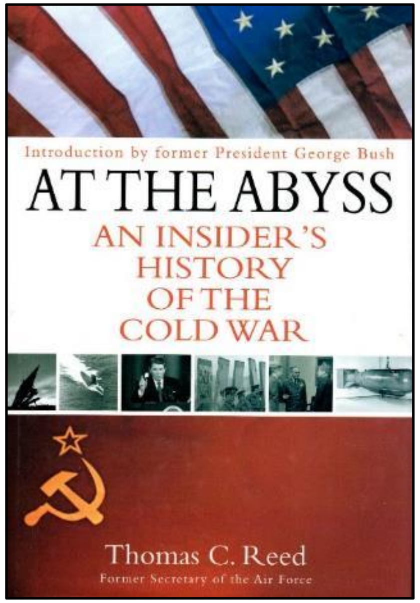
Pgs. 266-269

<u>NSC's Dr. Guss Weiss (1982)</u>

Why not help the Soviets with their shopping?

Now that we know what they want, we can "help" them get it.

At the Abyss


Introduction by former President George Bush
AT THE ABYSS
AN INSIDER'S HISTORY OF THE COLD WAR
Thomas C. Reed
Former Secretary of the Air Force

Pgs. 266-269

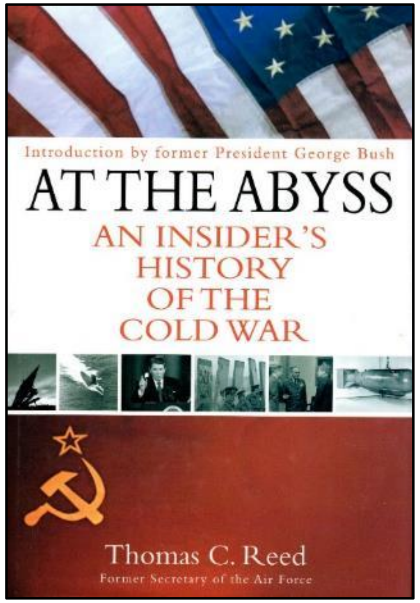
The CIA added *extra ingredients* to KGB hardware and software shopping items.

Improved (i.e. erratic) chip designs passed initial quality tests but sporadically failed in Soviet military-industrial applications.

Pseudosoftware disrupted factory output.

Flawed weapon designs went to Soviet Military Design Ministries.

At the Abyss



Introduction by former President George Bush
AT THE ABYSS
AN INSIDER'S HISTORY OF THE COLD WAR
Thomas C. Reed
Former Secretary of the Air Force

Pgs. 266-269

<u>Urengoi Gas Field Trans-Siberian Pipeline</u>

Soviets had bought early computer models on the open market.

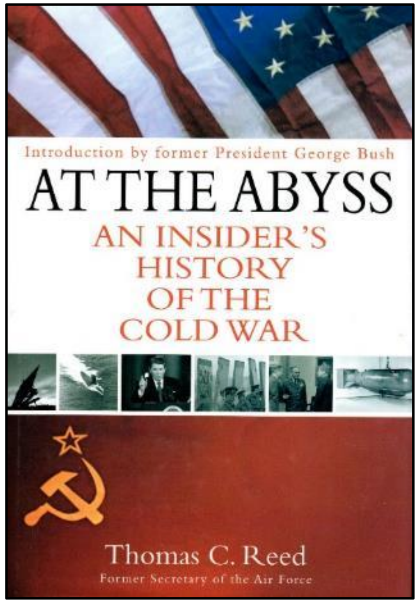
Valves, compressors, and storage facilities required sophisticated control software.

The USA denied the Soviets USA software.

Soviets attempted to steal the software from a Canadian company.

The CIA ensured the Soviets stole *improved* code with a *Trojan Horse* that ran beautifully *for a while*.

At the Abyss

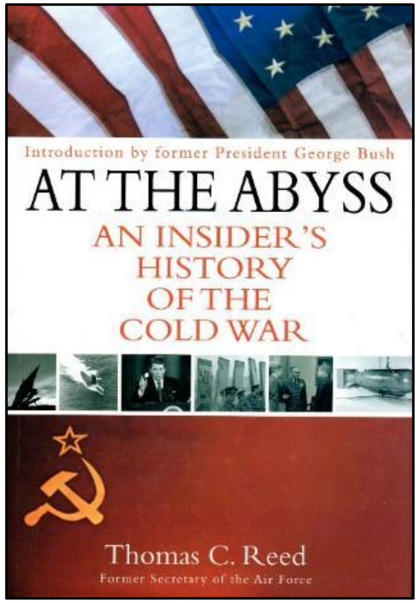

Introduction by former President George Bush
AT THE ABYSS
AN INSIDER'S HISTORY OF THE COLD WAR
Thomas C. Reed
Former Secretary of the Air Force

Pgs. 266-269

Urengoi Gas Field Trans-Siberian Pipeline

> … *the software that was to run the pumps, turbines, and valves was programmed to go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to the pipeline joints and welds.*

At the Abyss


Introduction by former President George Bush
AT THE ABYSS
AN INSIDER'S HISTORY OF THE COLD WAR
Thomas C. Reed
Former Secretary of the Air Force

Pgs. 266-269

<u>Urengoi Gas Field Trans-Siberian Pipeline</u>

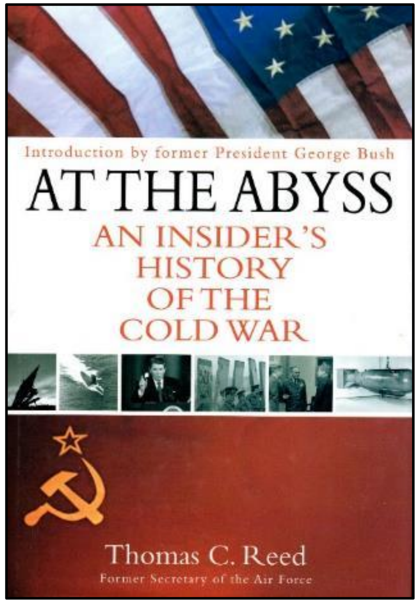
… *the most monumental non-nuclear explosion and fire ever seen from space*.

~ Three Kilotons. (20% - 25% Hiroshima Blast)

NORAD – *Missile liftoff in the middle of nowhere*?

Air Force – *No Electromagnetic Pulse (EMP)*?

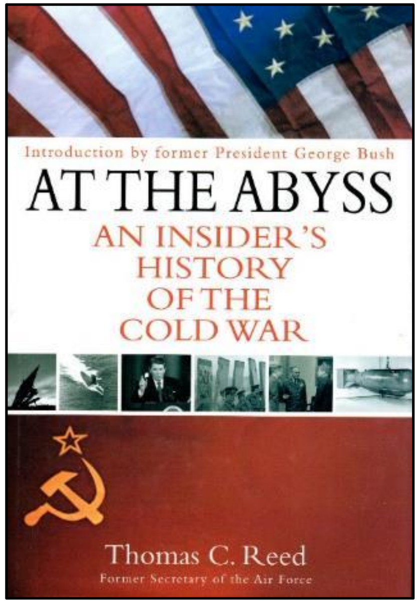
At the Abyss


Introduction by former President George Bush
AT THE ABYSS
AN INSIDER'S HISTORY OF THE COLD WAR
Thomas C. Reed
Former Secretary of the Air Force

Pgs. 266-269

Before these conflicting indicators turned into an international crisis, Guss Weiss came down the hall to tell his fellow NSC staffers not to worry.

At the Abyss

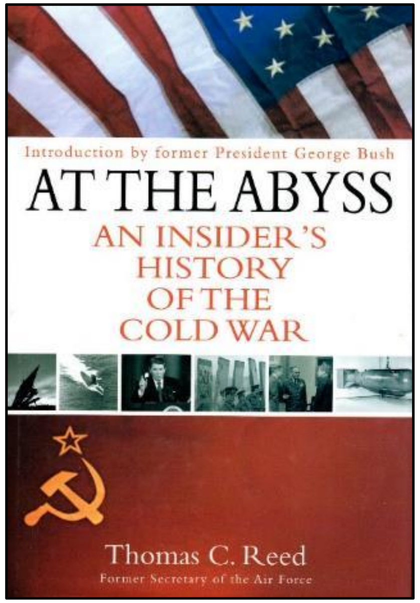

Introduction by former President George Bush
AT THE ABYSS
AN INSIDER'S HISTORY OF THE COLD WAR
Thomas C. Reed
Former Secretary of the Air Force

Pgs. 266-269

In time, the Soviets came to understand that they had been stealing bogus technology, but now what were they to do?

By implication, every cell of the Soviet technical leviathan might be affected.

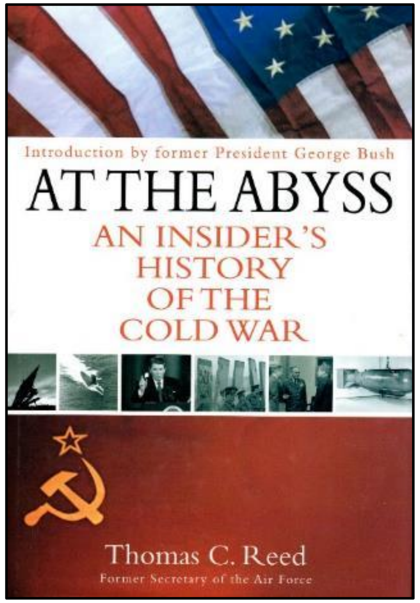
At the Abyss


Introduction by former President George Bush
AT THE ABYSS
AN INSIDER'S HISTORY OF THE COLD WAR
Thomas C. Reed
Former Secretary of the Air Force

Pgs. 266-269

… the Soviet electronics industry was infected with bugs, viruses, and Trojan Horses placed there by the U.S. intelligence community.

At the Abyss

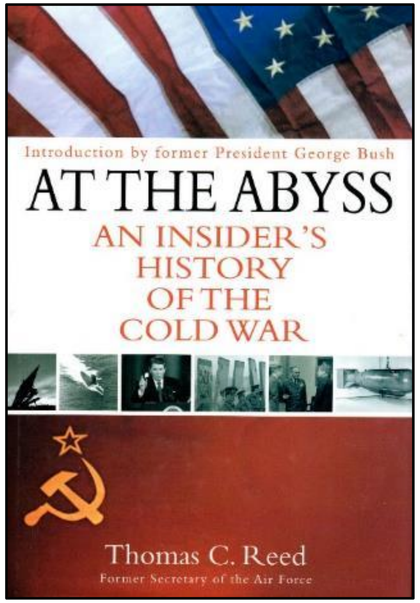

Introduction by former President George Bush
AT THE ABYSS
AN INSIDER'S HISTORY OF THE COLD WAR
Thomas C. Reed
Former Secretary of the Air Force

Pgs. 266-269

They had no way of knowing which equipment was sound, which was bogus.

All was suspect, which was the intended endgame for the entire operation.

At the Abyss



Introduction by former President George Bush

AT THE ABYSS

AN INSIDER'S HISTORY OF THE COLD WAR

Thomas C. Reed

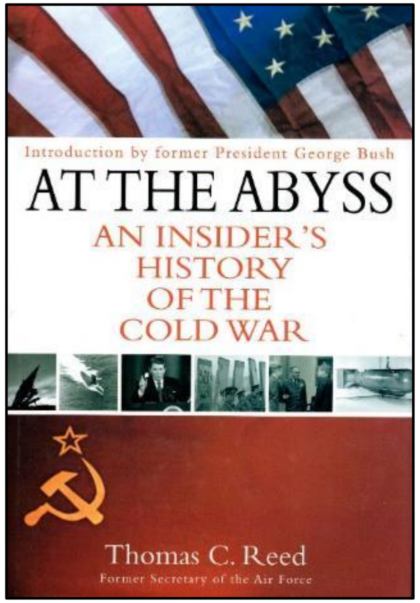
Former Secretary of the Air Force

Pgs. 266-269

There was significant damage to the Soviet economy.

Its ultimate bankruptcy, not a bloody battle or nuclear exchange, is what brought the Cold War to an end.

At the Abyss


Introduction by former President George Bush
AT THE ABYSS
AN INSIDER'S HISTORY OF THE COLD WAR
Thomas C. Reed
Former Secretary of the Air Force

Pgs. 266-269

As a grand finale, in 1984-85 the U.S. and its NATO allies rolled up the entire Line X collection network, both in the U.S. and overseas.

This effectively extinguished the KGB's technology collection capabilities at a time when Moscow was being sandwiched between a failing economy on one hand and an American President – intent on prevailing and ending the Cold War – on the other.

Farewell Dossier Post Mortem Analysis

Supply Chain Control?

Software Bill of Materials?

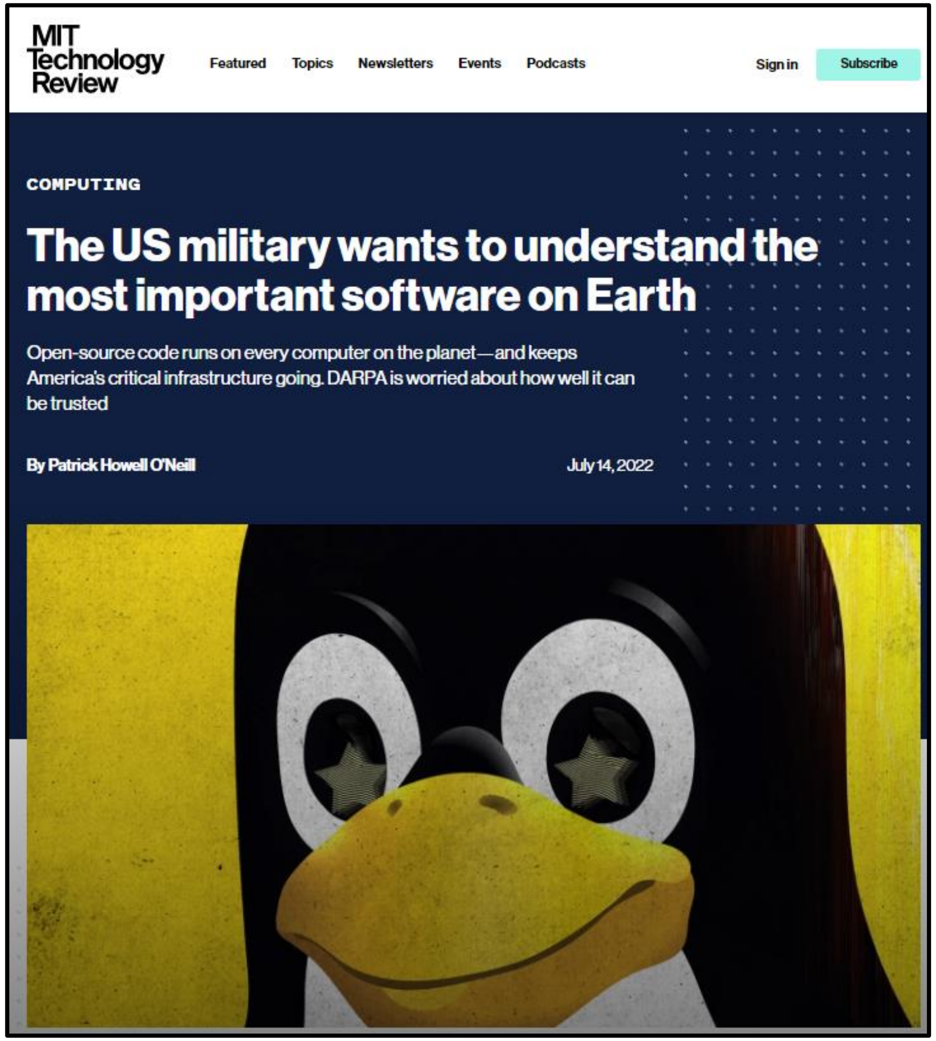
It has been said that history repeats itself.

This is perhaps not quite correct; it merely rhymes.

– Theodor Reik
The Unreachables

Software Bill of Materials?

7/14/2022



COMPUTING

The US military wants to understand the most important software on Earth

Open-source code runs on every computer on the planet—and keeps America's critical infrastructure going. DARPA is worried about how well it can be trusted

By Patrick Howell O'Neill

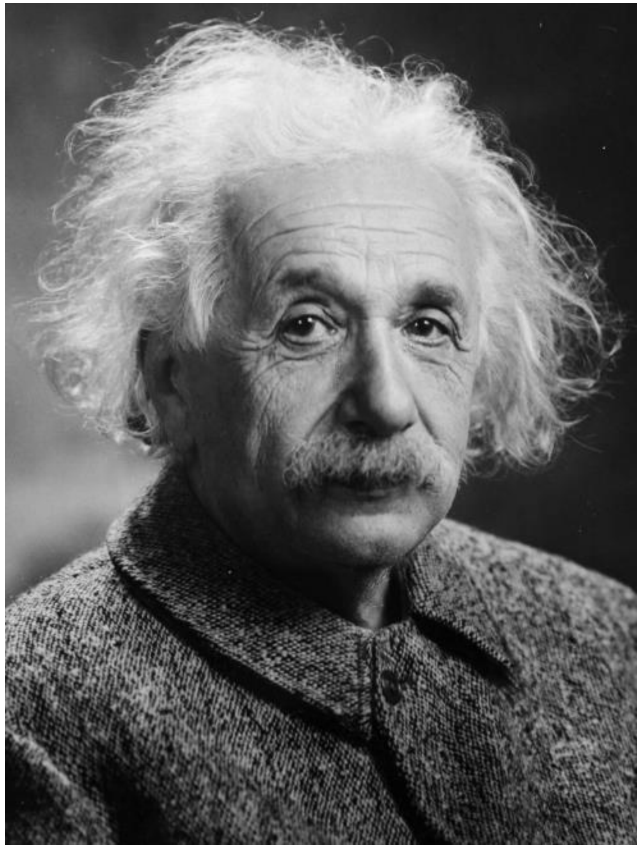
July 14, 2022

Linux & Open Source

There are countless software projects, millions of lines of code, numerous mailing lists and forums, and an ocean of contributors whose identities and motivation are often obscure, making it hard to hold them accountable.

HTTPS://WWW.TECHNOLOGYREVIEW.COM/2022/07/14/1055894/US-MILITARY-SOFWARE-LINUX-KERNEL-OPEN-SOURCE/

Software Bill of Materials?



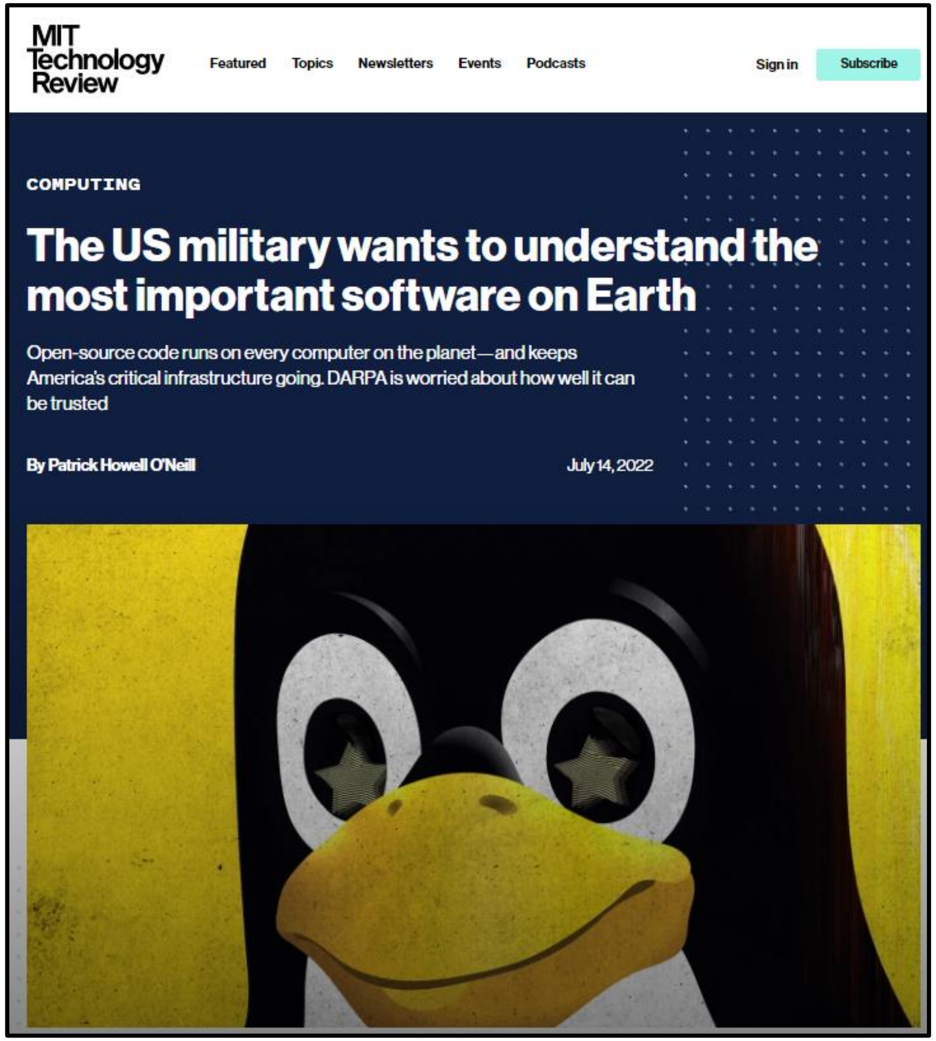
Never said it.

Half the world is below average,
some of them are
open source programmers.

https://commons.wikimedia.org/wiki/Category:Albert_Einstein#/media/File:Albert_Einstein_Head.jpg

Software Bill of Materials?

7/14/2022



COMPUTING

The US military wants to understand the most important software on Earth

Open-source code runs on every computer on the planet—and keeps America's critical infrastructure going. DARPA is worried about how well it can be trusted

By Patrick Howell O'Neill

July 14, 2022

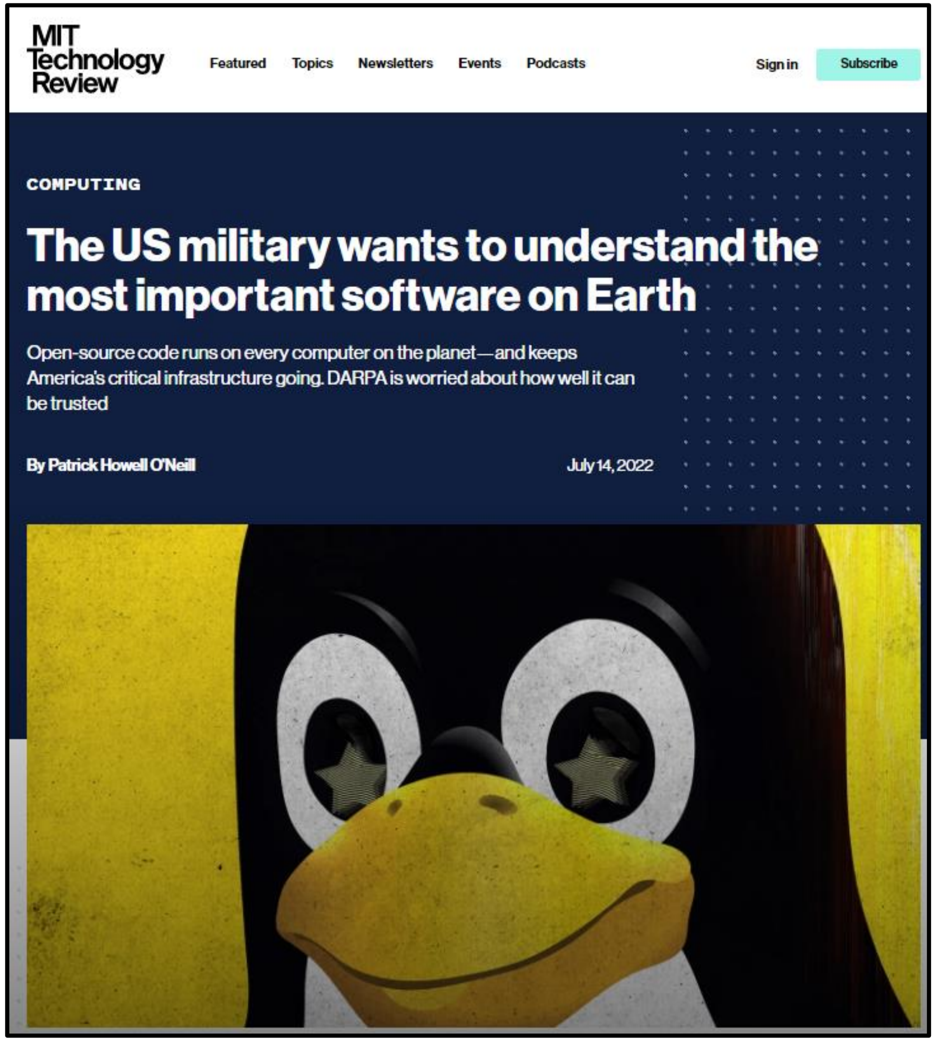
Linux & Open Source

For example, hackers have quietly inserted malicious code into open-source projects numerous times in recent years. Back doors can long escape detection, and, in the worst case, entire projects have been handed over to bad actors who take advantage of the trust people place in open-source communities and code. Sometimes there are disruptions or even takeovers of the very social networks that these projects depend on. Tracking it all has been mostly—though not entirely—a manual effort, which means it does not match the astronomical size of the problem.

HTTPS://WWW.TECHNOLOGYREVIEW.COM/2022/07/14/1055894/US-MILITARY-SOFWARE-LINUX-KERNEL-OPEN-SOURCE/

Software Bill of Materials?

7/14/2022



COMPUTING

The US military wants to understand the most important software on Earth

Open-source code runs on every computer on the planet—and keeps America's critical infrastructure going. DARPA is worried about how well it can be trusted

By Patrick Howell O'Neill

July 14, 2022

Linux & Open Source

"This is a core technology to our society. Not understanding kernel security means we can't secure critical infrastructure."

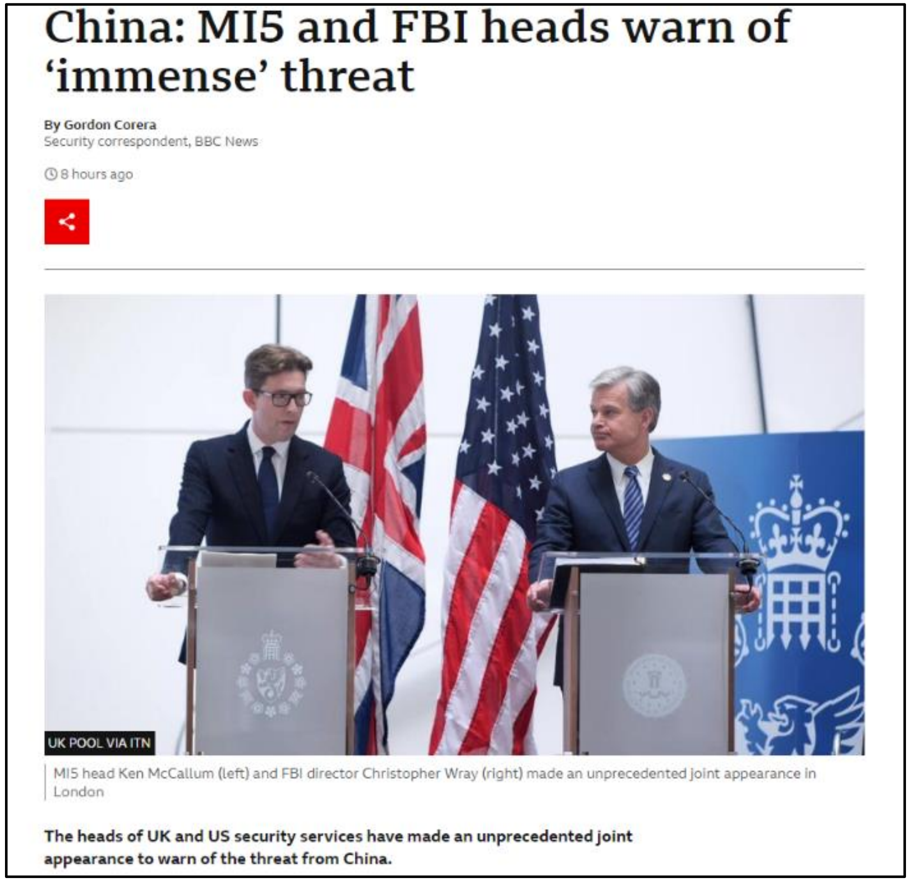
HTTPS://WWW.TECHNOLOGYREVIEW.COM/2022/07/14/1055894/US-MILITARY-SOFWARE-LINUX-KERNEL-OPEN-SOURCE/

Edward Weston

https://en.wikipedia.org/wiki/Edward_Weston#/media/File:Young_Edward_Weston_with_a_camera.jpg

The world is full of sloppy bohemians and their work betrays them.

FBI/MI6 China Warning – 07/07/2022



China: MI5 and FBI heads warn of 'immense' threat

By Gordon Corera
Security correspondent, BBC News

8 hours ago

MI5 head Ken McCallum (left) and FBI director Christopher Wray (right) made an unprecedented joint appearance in London

The heads of UK and US security services have made an unprecedented joint appearance to warn of the threat from China.

https://www.bbc.com/news/world-asia-china-62064506

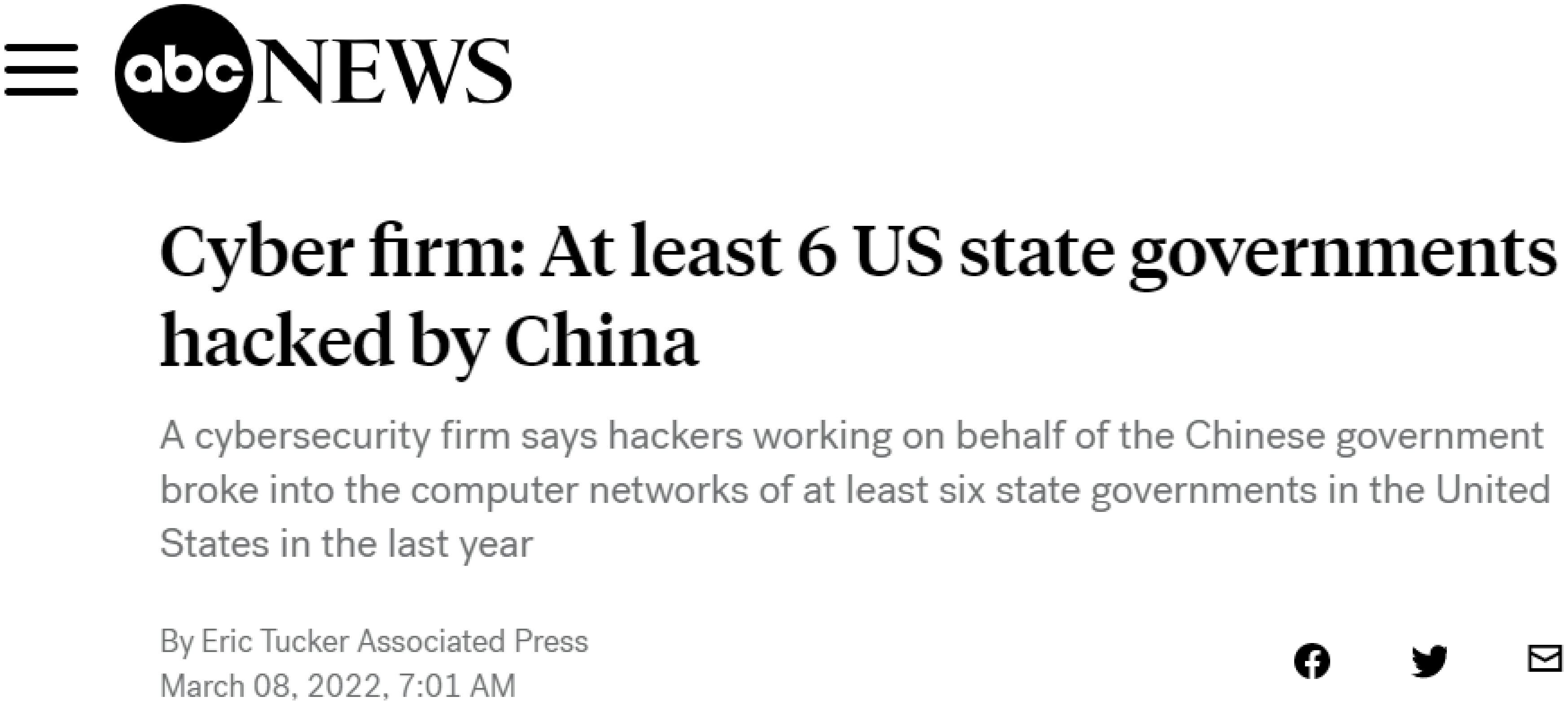
07/07/2022

McCallum: a *game-changing* challenge

Wray: *immense, breath-taking*

Wray: The Chinese government

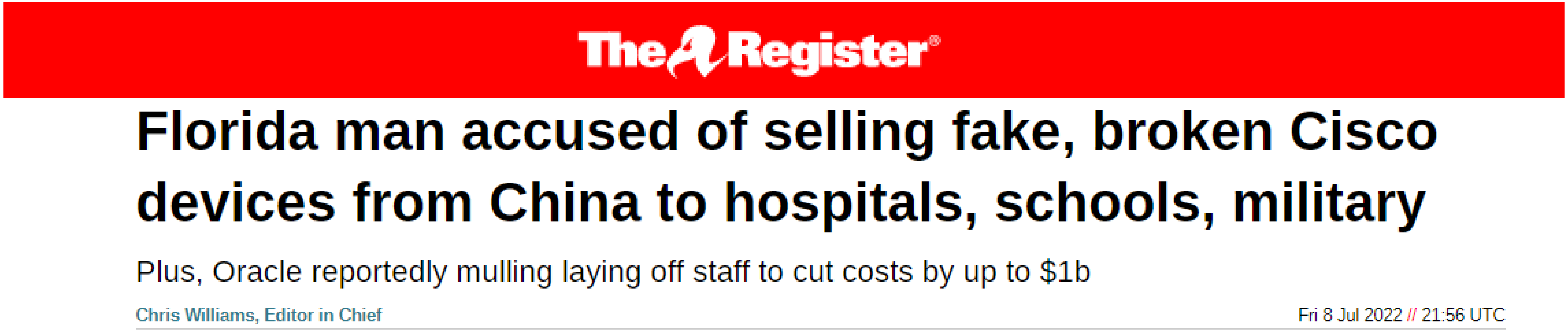
- *Has* a *hacking program larger than every other major country combined*
- Has deployed cyber espionage to *cheat and steal on a massive scale*
- Poses *an even more serious threat to western businesses than many sophisticated business people realize*.
- Is *set on stealing your technology*



Cyber firm: At least 6 US state governments hacked by China

A cybersecurity firm says hackers working on behalf of the Chinese government broke into the computer networks of at least six state governments in the United States in the last year

By Eric Tucker Associated Press
March 08, 2022, 7:01 AM



The Register®

Florida man accused of selling fake, broken Cisco devices from China to hospitals, schools, military

Plus, Oracle reportedly mulling laying off staff to cut costs by up to $1b

Chris Williams, Editor in Chief

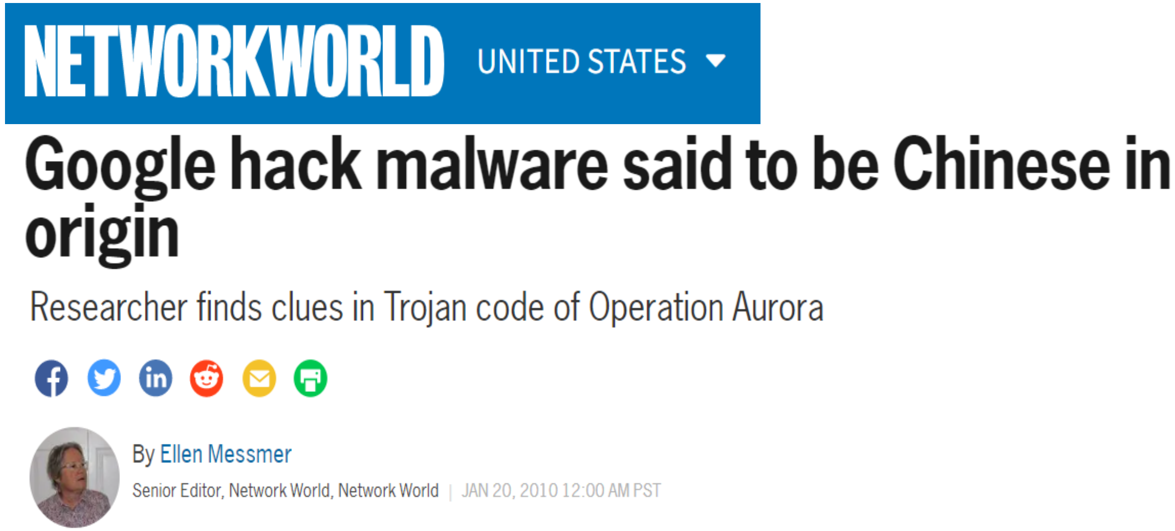
Fri 8 Jul 2022 // 21:56 UTC

These machines were, it is claimed, packaged up and sealed with fake Cisco labels and stickers, manuals, and other materials to make it all look above board. These boxes were then imported from the Middle Kingdom into the United States by Aksoy's Pro Network of companies, which then sold the bogus gear to hospitals, schools, government agencies, the military, and other customers, it is alleged.

And, it is claimed, these systems would just fail completely or not work correctly, disrupting computer networks and operations and costing users tens of thousands of dollars to correct.

https://www.theregister.com/2022/07/08/cisco_china_import_charges/

1/20/2010



NETWORKWORLD UNITED STATES

Google hack malware said to be Chinese in origin

Researcher finds clues in Trojan code of Operation Aurora

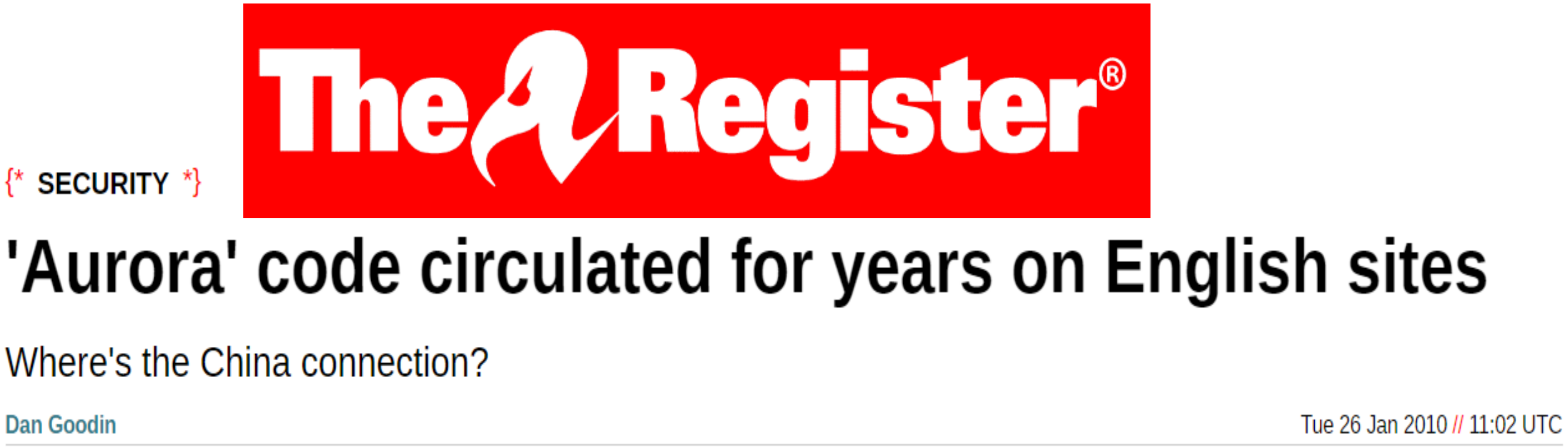
By Ellen Messmer

Senior Editor, Network World, Network World | JAN 20, 2010 12:00 AM PST

In examining the Hydraq Trojan in the malware code, Stewart found it uses a 16-bit CRC implementation that shows the source-code sample "is of Chinese origin, released as part of a Chinese-language paper on optimizing CRC algorithms for use in controllers.“

This CRC algorithm "seems to be virtually unknown outside of China," Stewart's paper states. "This information strongly indicates the Aurora codebase originated with someone who is comfortable reading simplified Chinese." Although source code is not restrained by any human language or nationality, most programmers will reuse code documented in their native language since to do otherwise "is to invite bugs and other unexpected problems" from misunderstanding of the source code's purpose, the SecureWorks paper says.

https://www.networkworld.com/article/2243018/google-hack-malware-said-to-be-chinese-in-origin.html



{* SECURITY *}

The Register®

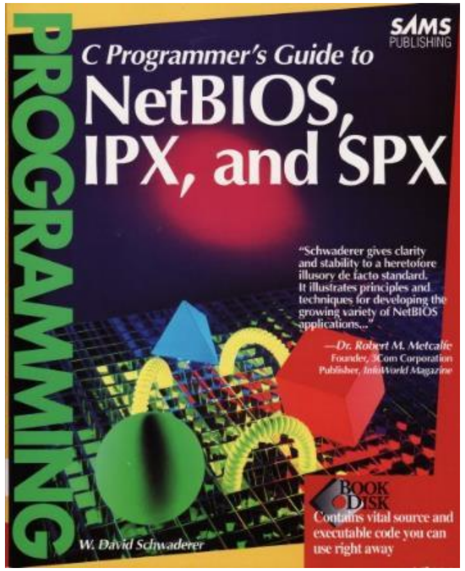
'Aurora' code circulated for years on English sites

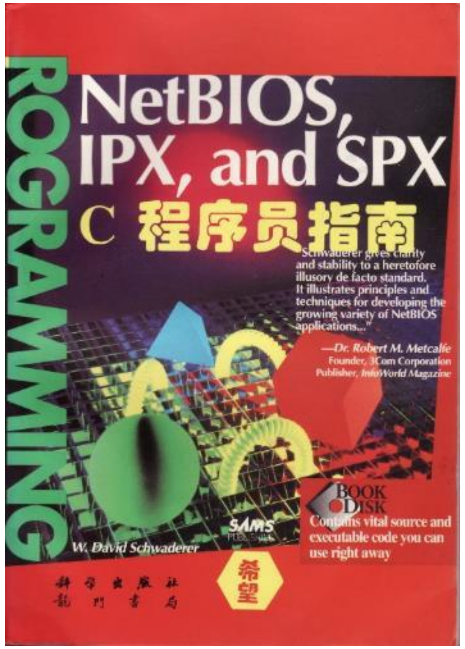
Where's the China connection?

Dan Goodin

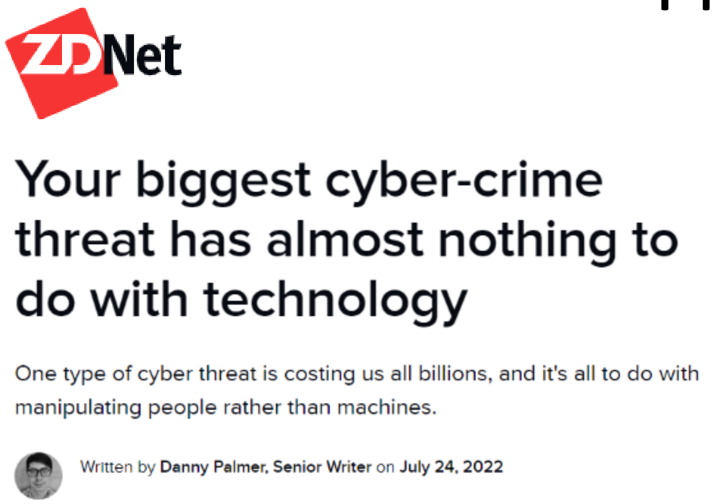
Tue 26 Jan 2010 // 11:02 UTC

The method was also discussed in W. David Schwaderer's 1988 book C Programmer's Guide to NetBIOS. On page 200, it refers to a CRC approach that "only requires 16 unsigned integers that occupy a mere 32 bytes in a typical machine." On page 205, the author goes on to provide source code that's very similar to the Aurora algorithm.


SAMS PUBLISHING
C Programmer's Guide to
NetBIOS, IPX, and SPX
PROGRAMMING
"Schwaderer gives clarity and stability to a heretofore illusory de facto standard. It illustrates principles and techniques for developing the growing variety of NetBIOS applications..."
—Dr. Robert M. Metcalfe Founder, 3Com Corporation Publisher, InfoWorld Magazine
BOOK DISK
Contains vital source and executable code you can use right away
W. David Schwaderer


NetBIOS, IPX, and SPX
C 程序员指南
PROGRAMMING
Schwaderer gives clarity and stability to a heretofore illusory de facto standard. It illustrates principles and techniques for developing the growing variety of NetBIOS applications...
—Dr. Robert M. Metcalfe Founder, 3Com Corporation Publisher, InfoWorld Magazine
BOOK DISK
Contains vital source and executable code you can use right away
SAMS
W. David Schwaderer
希望

The Human Element



ZDNet

Your biggest cyber-crime threat has almost nothing to do with technology

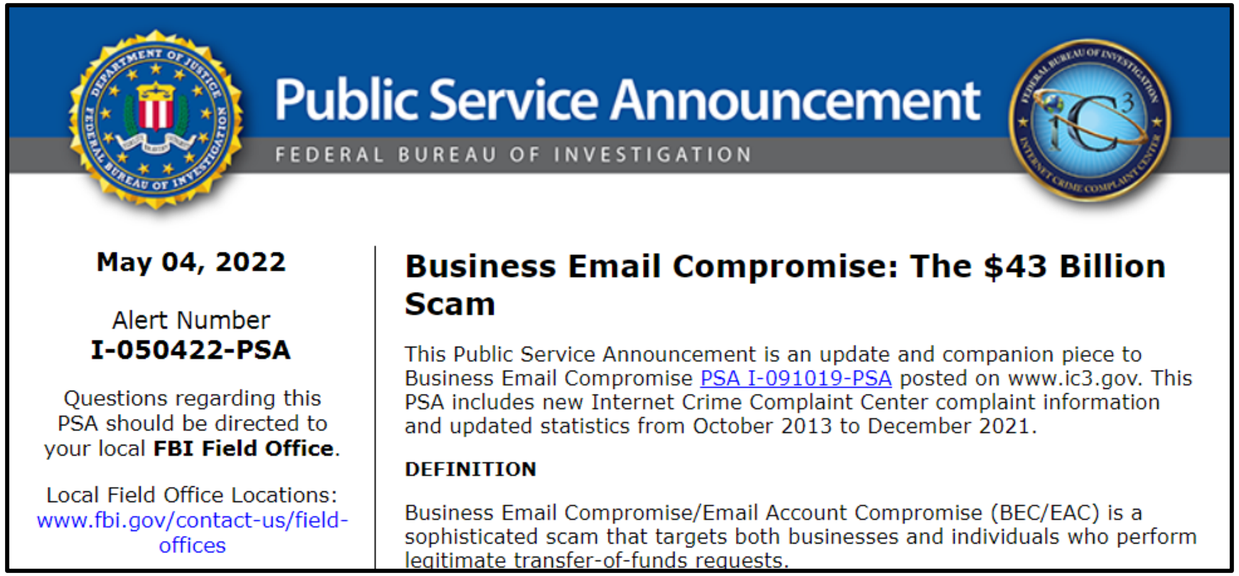
One type of cyber threat is costing us all billions, and it's all to do with manipulating people rather than machines.

Written by **Danny Palmer, Senior Writer** on **July 24, 2022**

https://www.zdnet.com/article/your-biggest-cyber-crime-threat-has-almost-nothing-to-do-with-technology/

BEC is a global problem. … reported in all 50 US states and by victims in 177 countries. …

… a sophisticated ruse that targets business and individuals who are duped into transferring funds to the scammer's account under the belief they are performing a legitimate transaction. …



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

May 04, 2022

Alert Number
I-050422-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field-offices

Business Email Compromise: The $43 Billion Scam

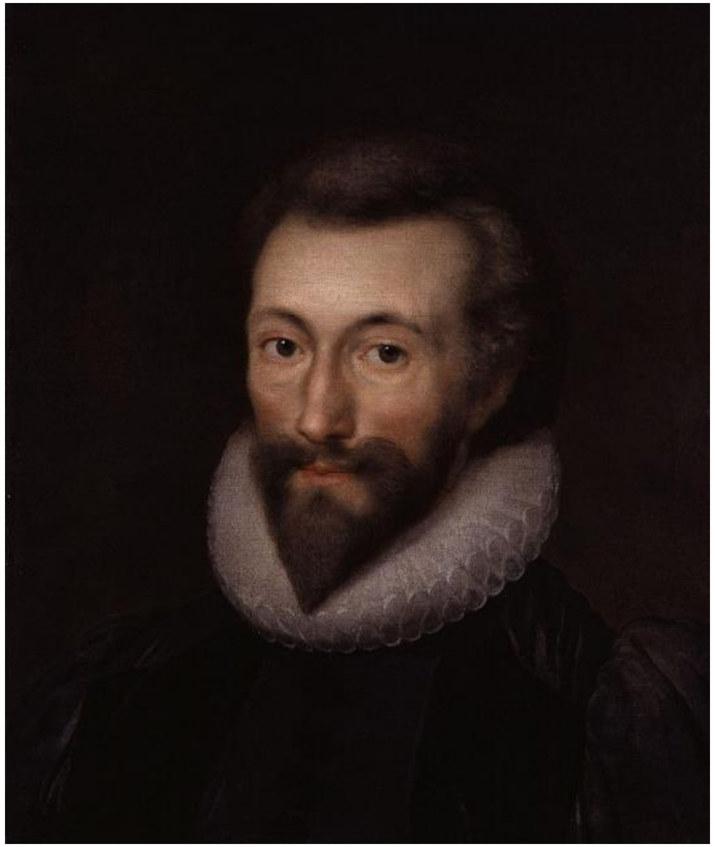
This Public Service Announcement is an update and companion piece to Business Email Compromise PSA I-091019-PSA posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center complaint information and updated statistics from October 2013 to December 2021.

DEFINITION

Business Email Compromise/Email Account Compromise (BEC/EAC) is a sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests.

https://www.ic3.gov/Media/Y2022/PSA220504

The Situation is Serious



… *never send to know for whom*
the bell tolls;
it tolls for thee.
– John Donne
Devotions upon Emergent Occasions, 1624

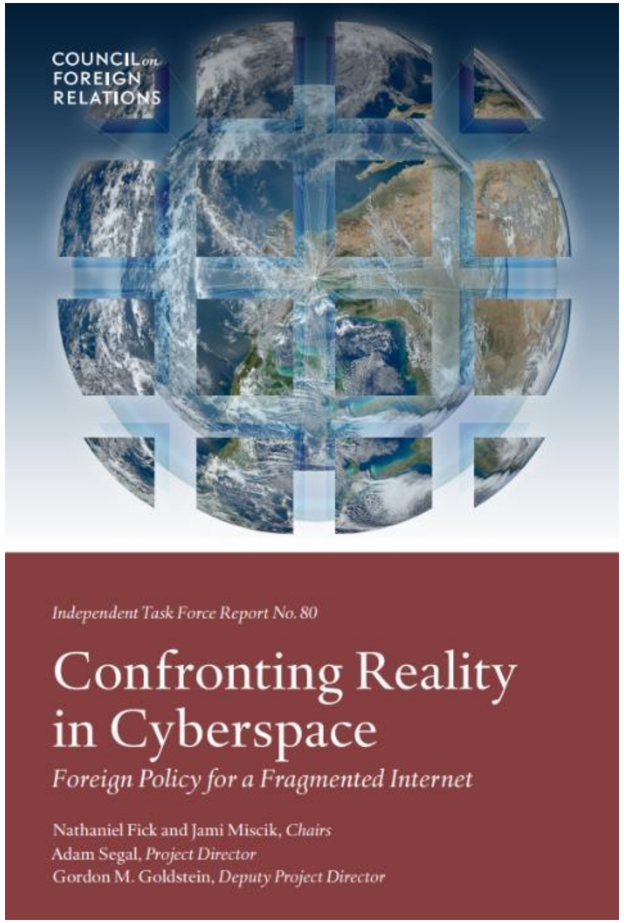
It’s not just business.

It’s personal.

It’s serious.

Council on Foreign Relations Report

July 12, 2022



COUNCIL on FOREIGN RELATIONS

Independent Task Force Report No. 80

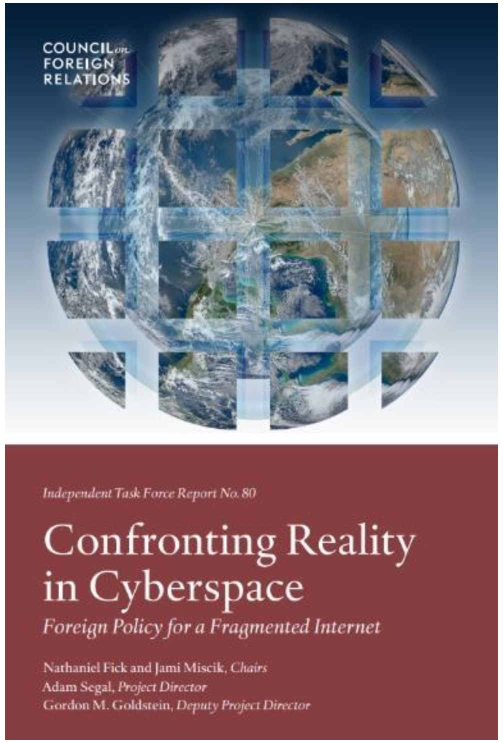
Confronting Reality in Cyberspace

Foreign Policy for a Fragmented Internet

Nathaniel Fick and Jami Miscik, *Chairs*
Adam Segal, *Project Director*
Gordon M. Goldstein, *Deputy Project Director*

https://www.cfr.org/report/confronting-reality-in-cyberspace/download/pdf/2022-07/CFR_TFR80_Cyberspace_Full_SinglePages_06212022_Final.pdf

Council on Foreign Relations Report



COUNCIL on FOREIGN RELATIONS

Independent Task Force Report No. 80

Confronting Reality in Cyberspace

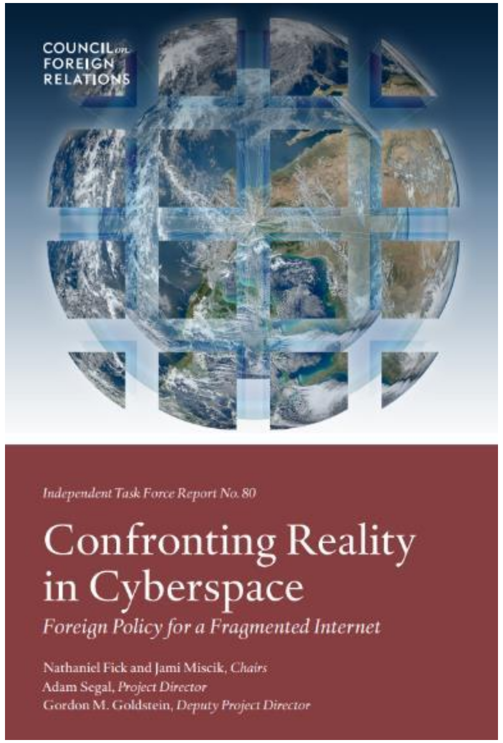
Foreign Policy for a Fragmented Internet

Nathaniel Fick and Jami Miscik, *Chairs*
Adam Segal, *Project Director*
Gordon M. Goldstein, *Deputy Project Director*

July 12, 2022

The utopian vision of an open, reliable, and secure global network has not been achieved and is unlikely ever to be realized. Today, the internet is less free, more fragmented, and less secure.

Council on Foreign Relations Report



COUNCIL *on* FOREIGN RELATIONS

Independent Task Force Report No. 80

Confronting Reality in Cyberspace

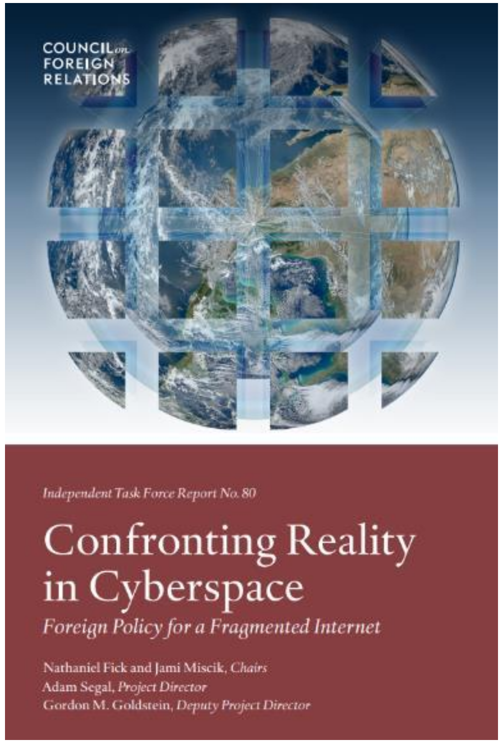
Foreign Policy for a Fragmented Internet

Nathaniel Fick and Jami Miscik, *Chairs*
Adam Segal, *Project Director*
Gordon M. Goldstein, *Deputy Project Director*

July 12, 2022

The lack of regulation around something so integral to modern economies, societies, political systems, and militaries has also become dangerous. This openness presents a tempting target for both states and nonstate actors seeking to undermine democracy, promote terrorism, steal intellectual property, and cause extraordinary disruption.

Council on Foreign Relations Report



COUNCIL on FOREIGN RELATIONS

Independent Task Force Report No. 80

Confronting Reality in Cyberspace

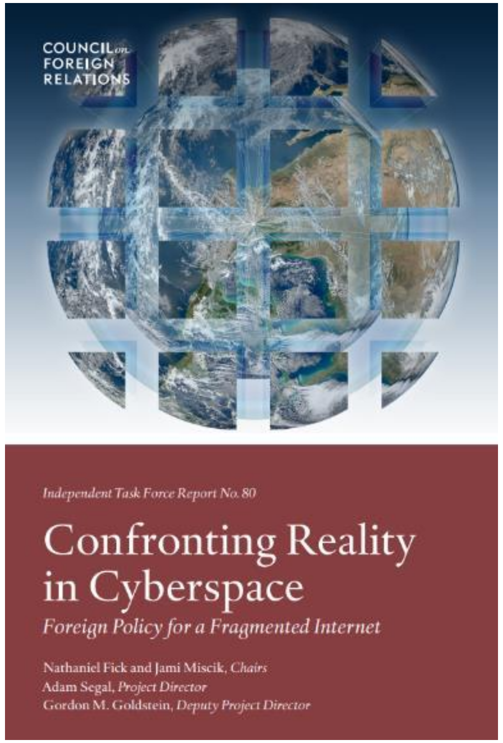
Foreign Policy for a Fragmented Internet

Nathaniel Fick and Jami Miscik, *Chairs*
Adam Segal, *Project Director*
Gordon M. Goldstein, *Deputy Project Director*

July 12, 2022

Even more dangerous is the vulnerability of critical infrastructure to cyberattacks. Making the circumstances all the more difficult, figuring out who is behind a given attack remains challenging, allowing states and nonstate actors to carry out cyberattacks with a high degree of deniability and avoid significant consequences.

Council on Foreign Relations Report



COUNCIL *on* FOREIGN RELATIONS

Independent Task Force Report No. 80

Confronting Reality in Cyberspace

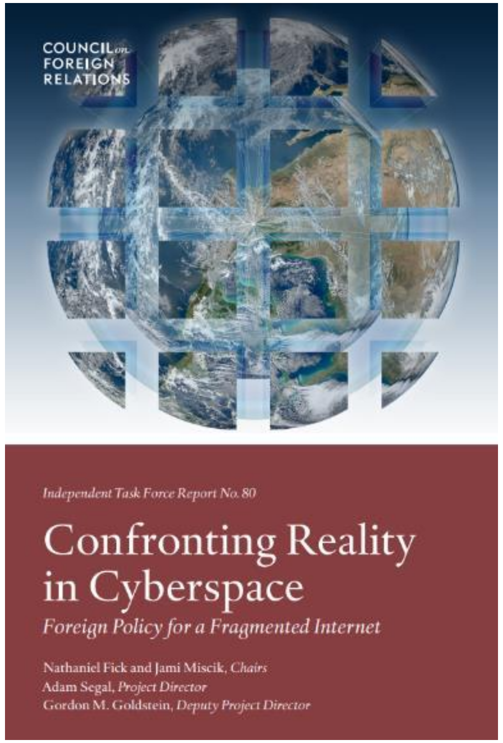
Foreign Policy for a Fragmented Internet

Nathaniel Fick and Jami Miscik, *Chairs*
Adam Segal, *Project Director*
Gordon M. Goldstein, *Deputy Project Director*

July 12, 2022

Frankly, U.S. policy toward cyberspace and the internet has failed to keep up. The United States desperately needs a new foreign policy that confronts head on the consequences of a fragmented and dangerous internet.

Council on Foreign Relations Report



COUNCIL on FOREIGN RELATIONS

Independent Task Force Report No. 80

Confronting Reality in Cyberspace

Foreign Policy for a Fragmented Internet

Nathaniel Fick and Jami Miscik, *Chairs*
Adam Segal, *Project Director*
Gordon M. Goldstein, *Deputy Project Director*

July 12, 2022

The Task Force concludes that—among other things—the era of the global internet is over; …
Cybercrime is a pressing national security threat; and Washington and its allies have failed to impose sufficient consequences on attackers.

What is Ransomware?

An exponentially growing, omni-present enterprise risk, where infected hosts exfiltrate [and optionally encrypt] business-critical data, holding it hostage until the victim pays the attacker an extortion ransom.

There are numerous ransomware varieties.

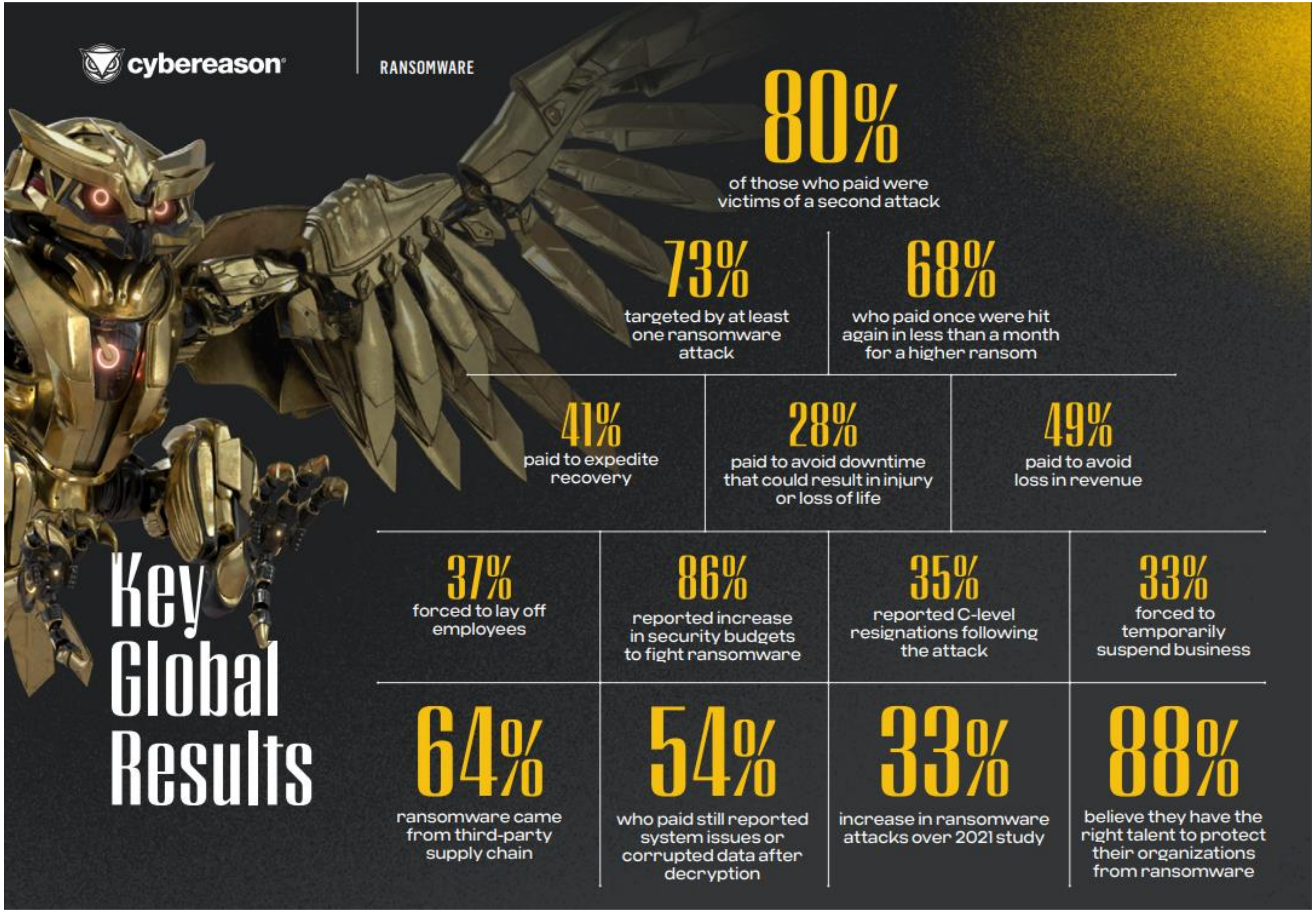
Attackers deploy ransomware through spearphishing campaigns, drive-by downloads, and through traditional remote service-based exploitations.

Ransomware and Cybersecurity are Inseparable Topics

Cybereason© Global Study on Ransomware Business Impact

cybereason
2022
Ransomware
The True Cost to Business
A Global Study on Ransomware Business Impact

https://www.cybereason.com/ransomware-the-true-cost-to-business-2022?



cybereason | RANSOMWARE

Key Global Results

80% of those who paid were victims of a second attack

73% targeted by at least one ransomware attack

68% who paid once were hit again in less than a month for a higher ransom

41% paid to expedite recovery

28% paid to avoid downtime that could result in injury or loss of life

49% paid to avoid loss in revenue

37% forced to lay off employees

86% reported increase in security budgets to fight ransomware

35% reported C-level resignations following the attack

33% forced to temporarily suspend business

64% ransomware came from third-party supply chain

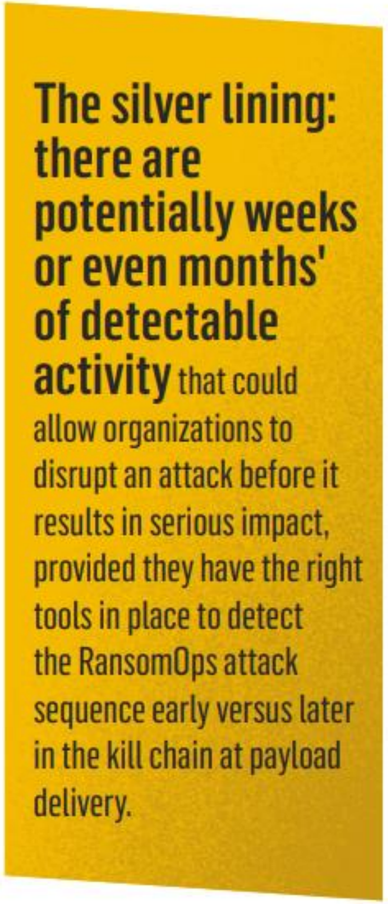
54% who paid still reported system issues or corrupted data after decryption

33% increase in ransomware attacks over 2021 study

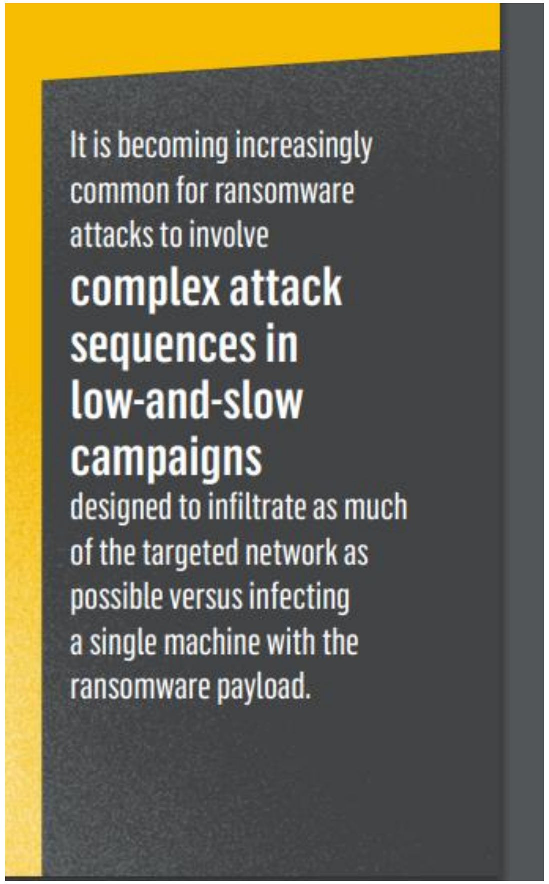
88% believe they have the right talent to protect their organizations from ransomware

https://www.cybereason.com/ransomware-the-true-cost-to-business-2022?

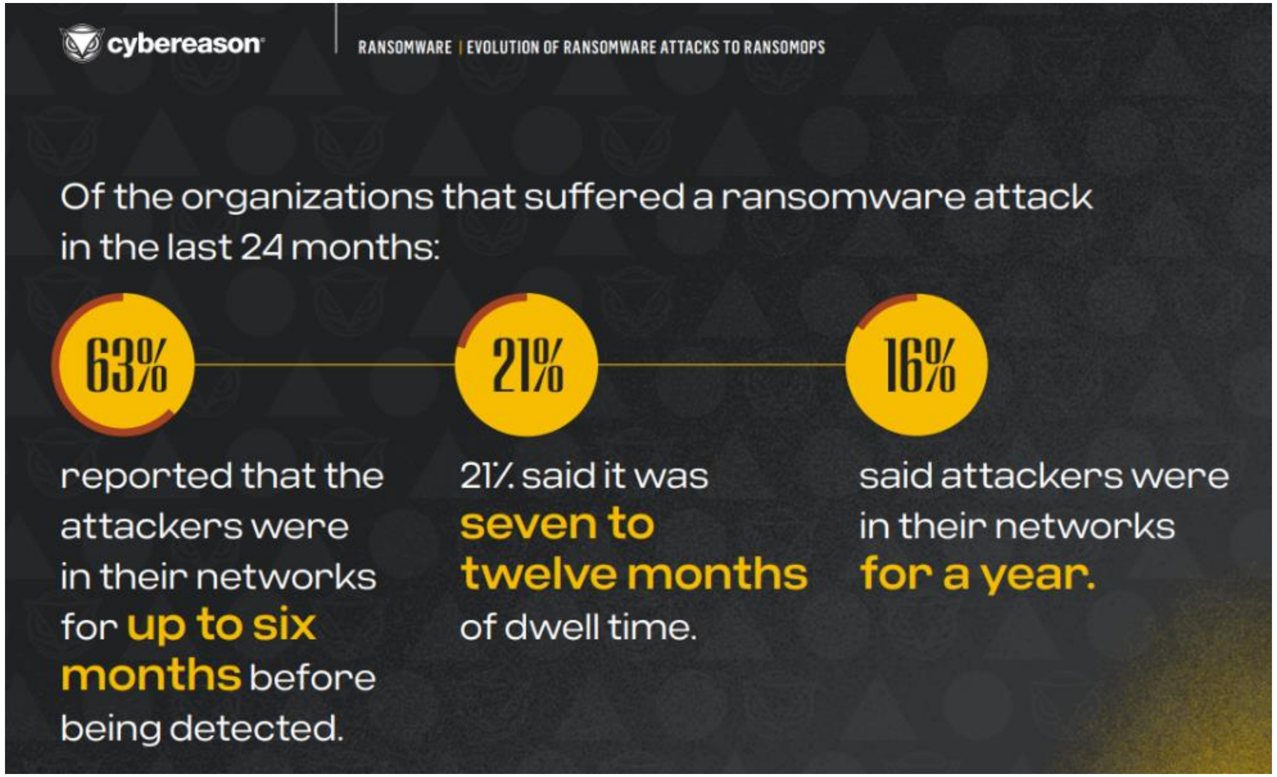
Ascent of *Zero Trust*



The silver lining: there are potentially weeks or even months' of detectable activity that could allow organizations to disrupt an attack before it results in serious impact, provided they have the right tools in place to detect the RansomOps attack sequence early versus later in the kill chain at payload delivery.



It is becoming increasingly common for ransomware attacks to involve **complex attack sequences in low-and-slow campaigns** designed to infiltrate as much of the targeted network as possible versus infecting a single machine with the ransomware payload.



cybereason | RANSOMWARE | EVOLUTION OF RANSOMWARE ATTACKS TO RANSOMOPS

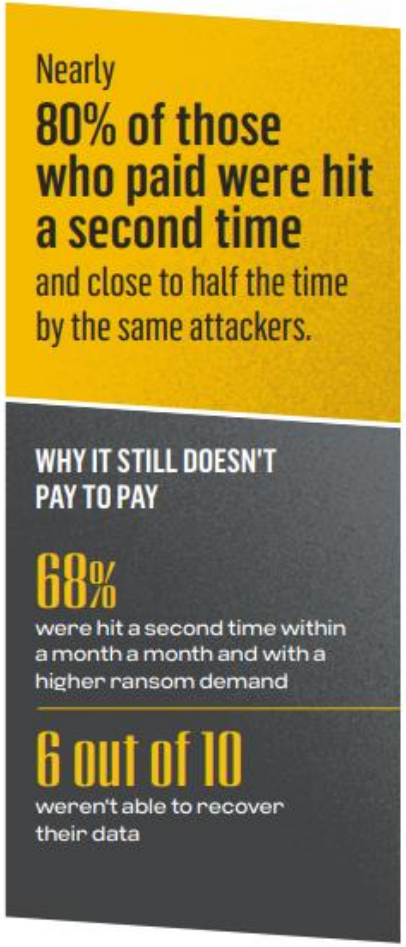
Of the organizations that suffered a ransomware attack in the last 24 months:

63% reported that the attackers were in their networks for **up to six months** before being detected.

21% 21٪ said it was **seven to twelve months** of dwell time.

16% said attackers were in their networks **for a year.**

https://www.cybereason.com/ransomware-the-true-cost-to-business-2022?

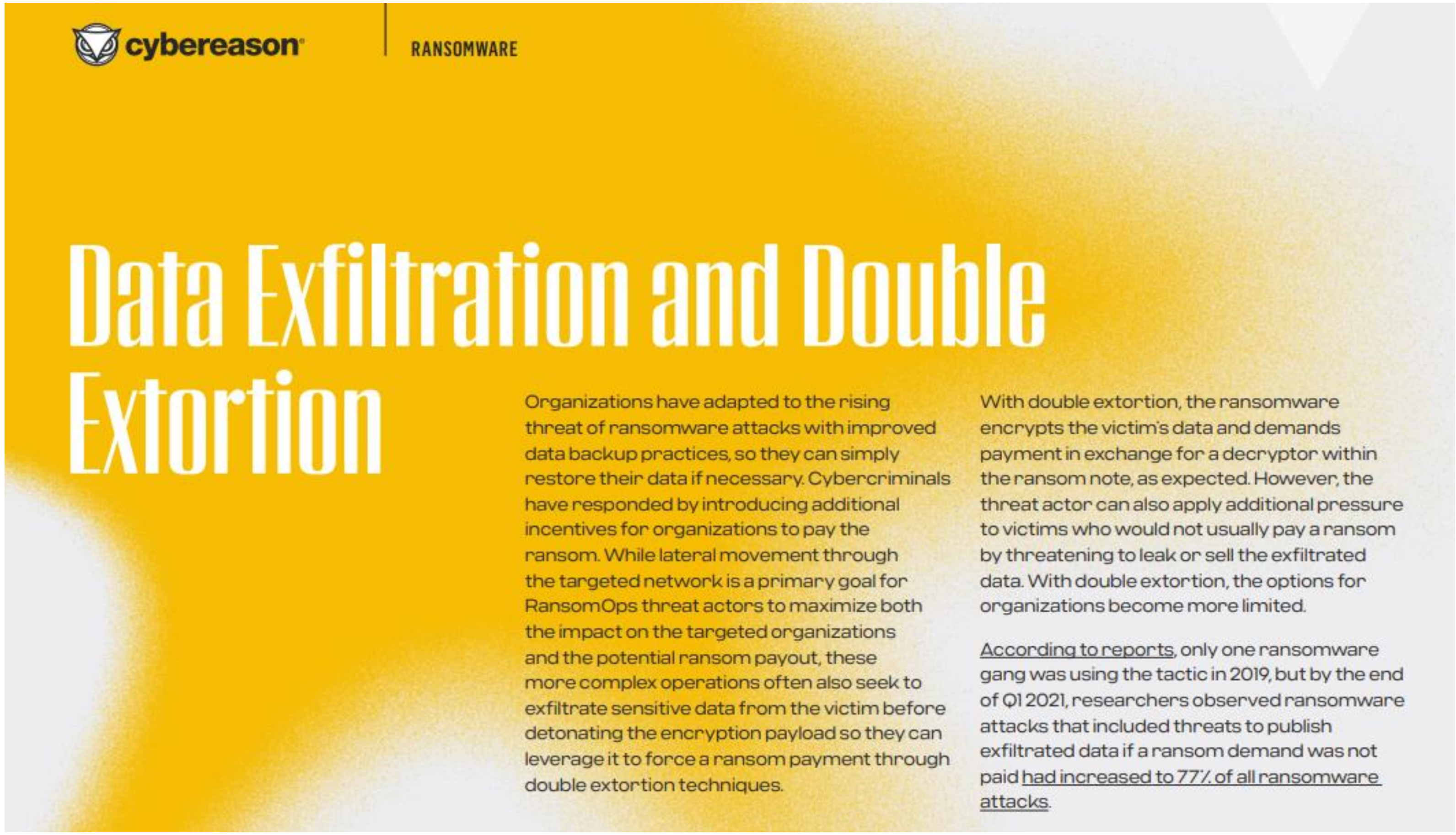


Nearly **80% of those who paid were hit a second time** and close to half the time by the same attackers.

WHY IT STILL DOESN'T PAY TO PAY

68%
were hit a second time within a month a month and with a higher ransom demand

6 out of 10
weren't able to recover their data



cybereason | RANSOMWARE

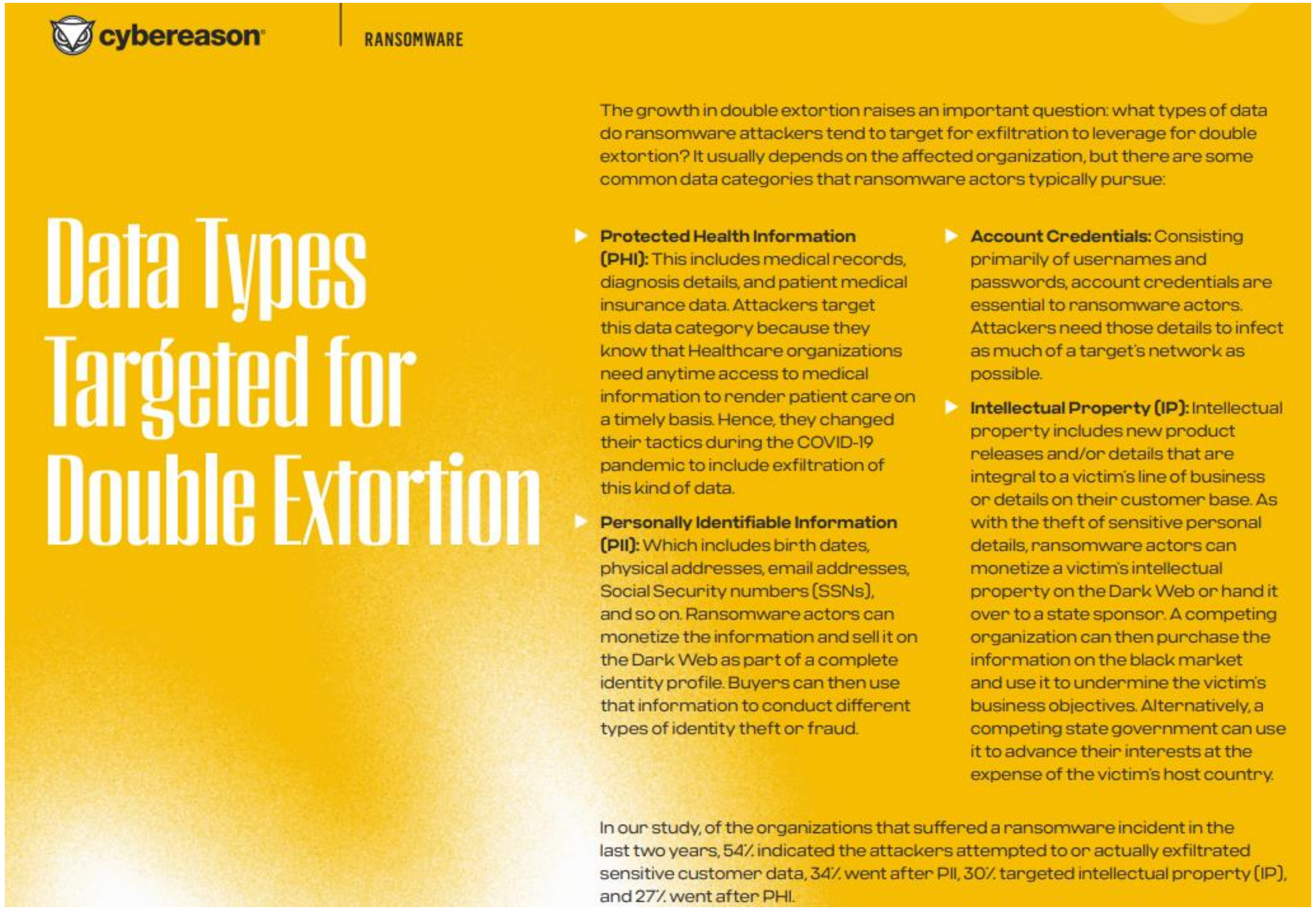
Data Exfiltration and Double Extortion

Organizations have adapted to the rising threat of ransomware attacks with improved data backup practices, so they can simply restore their data if necessary. Cybercriminals have responded by introducing additional incentives for organizations to pay the ransom. While lateral movement through the targeted network is a primary goal for RansomOps threat actors to maximize both the impact on the targeted organizations and the potential ransom payout, these more complex operations often also seek to exfiltrate sensitive data from the victim before detonating the encryption payload so they can leverage it to force a ransom payment through double extortion techniques.

With double extortion, the ransomware encrypts the victim's data and demands payment in exchange for a decryptor within the ransom note, as expected. However, the threat actor can also apply additional pressure to victims who would not usually pay a ransom by threatening to leak or sell the exfiltrated data. With double extortion, the options for organizations become more limited.

According to reports, only one ransomware gang was using the tactic in 2019, but by the end of Q1 2021, researchers observed ransomware attacks that included threats to publish exfiltrated data if a ransom demand was not paid had increased to 77% of all ransomware attacks.

https://www.cybereason.com/ransomware-the-true-cost-to-business-2022?



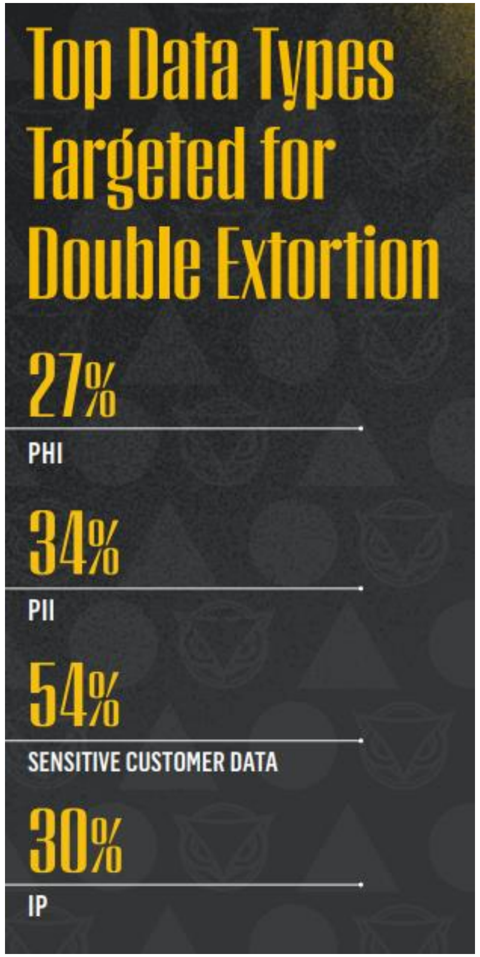
cybereason | RANSOMWARE

Data Types Targeted for Double Extortion

The growth in double extortion raises an important question: what types of data do ransomware attackers tend to target for exfiltration to leverage for double extortion? It usually depends on the affected organization, but there are some common data categories that ransomware actors typically pursue:

- **Protected Health Information (PHI):** This includes medical records, diagnosis details, and patient medical insurance data. Attackers target this data category because they know that Healthcare organizations need anytime access to medical information to render patient care on a timely basis. Hence, they changed their tactics during the COVID-19 pandemic to include exfiltration of this kind of data.
- **Personally Identifiable Information (PII):** Which includes birth dates, physical addresses, email addresses, Social Security numbers (SSNs), and so on. Ransomware actors can monetize the information and sell it on the Dark Web as part of a complete identity profile. Buyers can then use that information to conduct different types of identity theft or fraud.
- **Account Credentials:** Consisting primarily of usernames and passwords, account credentials are essential to ransomware actors. Attackers need those details to infect as much of a target's network as possible.
- **Intellectual Property (IP):** Intellectual property includes new product releases and/or details that are integral to a victim's line of business or details on their customer base. As with the theft of sensitive personal details, ransomware actors can monetize a victim's intellectual property on the Dark Web or hand it over to a state sponsor. A competing organization can then purchase the information on the black market and use it to undermine the victim's business objectives. Alternatively, a competing state government can use it to advance their interests at the expense of the victim's host country.

In our study, of the organizations that suffered a ransomware incident in the last two years, 54% indicated the attackers attempted to or actually exfiltrated sensitive customer data, 34% went after PII, 30% targeted intellectual property (IP), and 27% went after PHI.



Top Data Types Targeted for Double Extortion

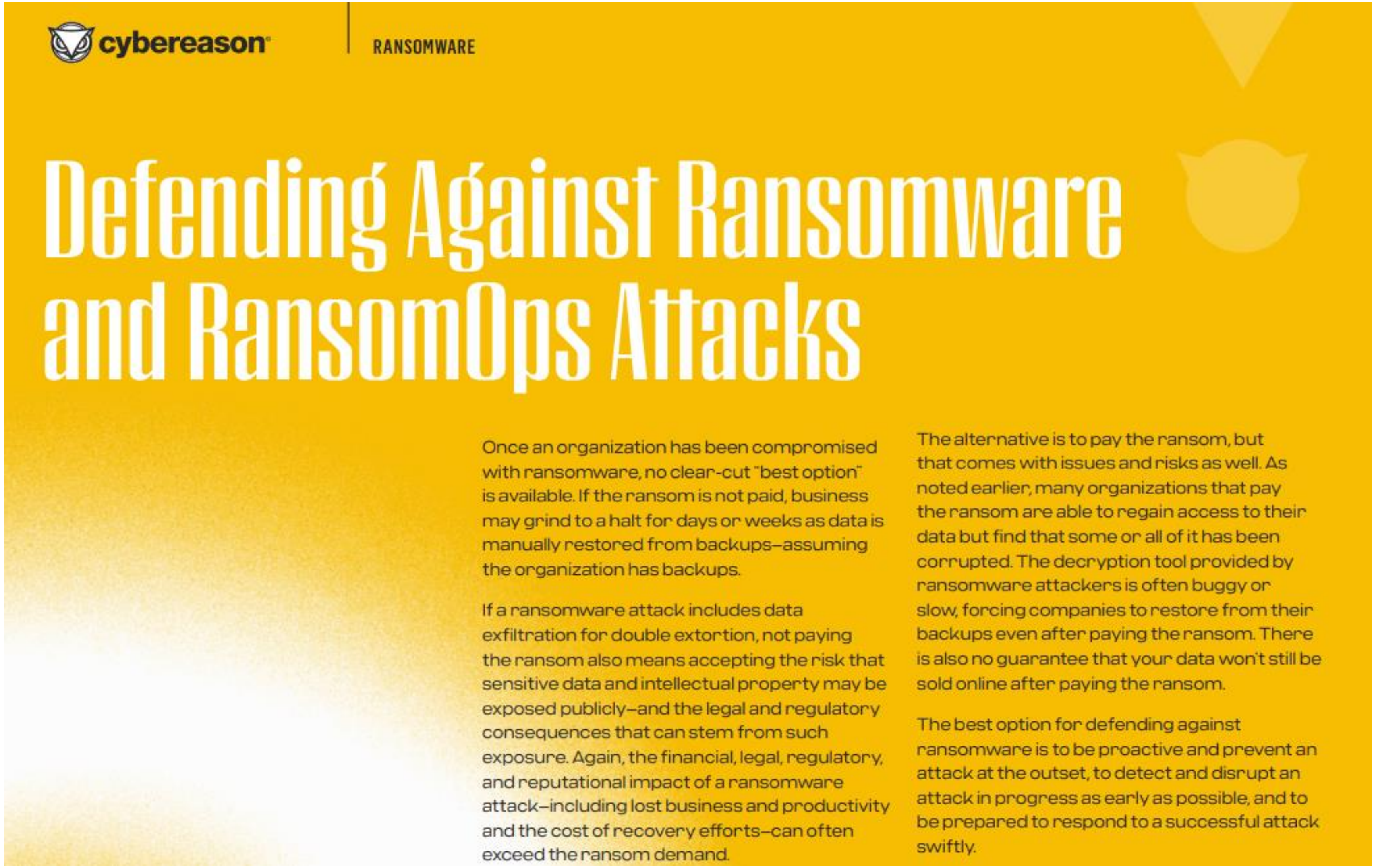
27%
PHI

34%
PII

54%
SENSITIVE CUSTOMER DATA

30%
IP

https://www.cybereason.com/ransomware-the-true-cost-to-business-2022?



cybereason | RANSOMWARE

Defending Against Ransomware and RansomOps Attacks

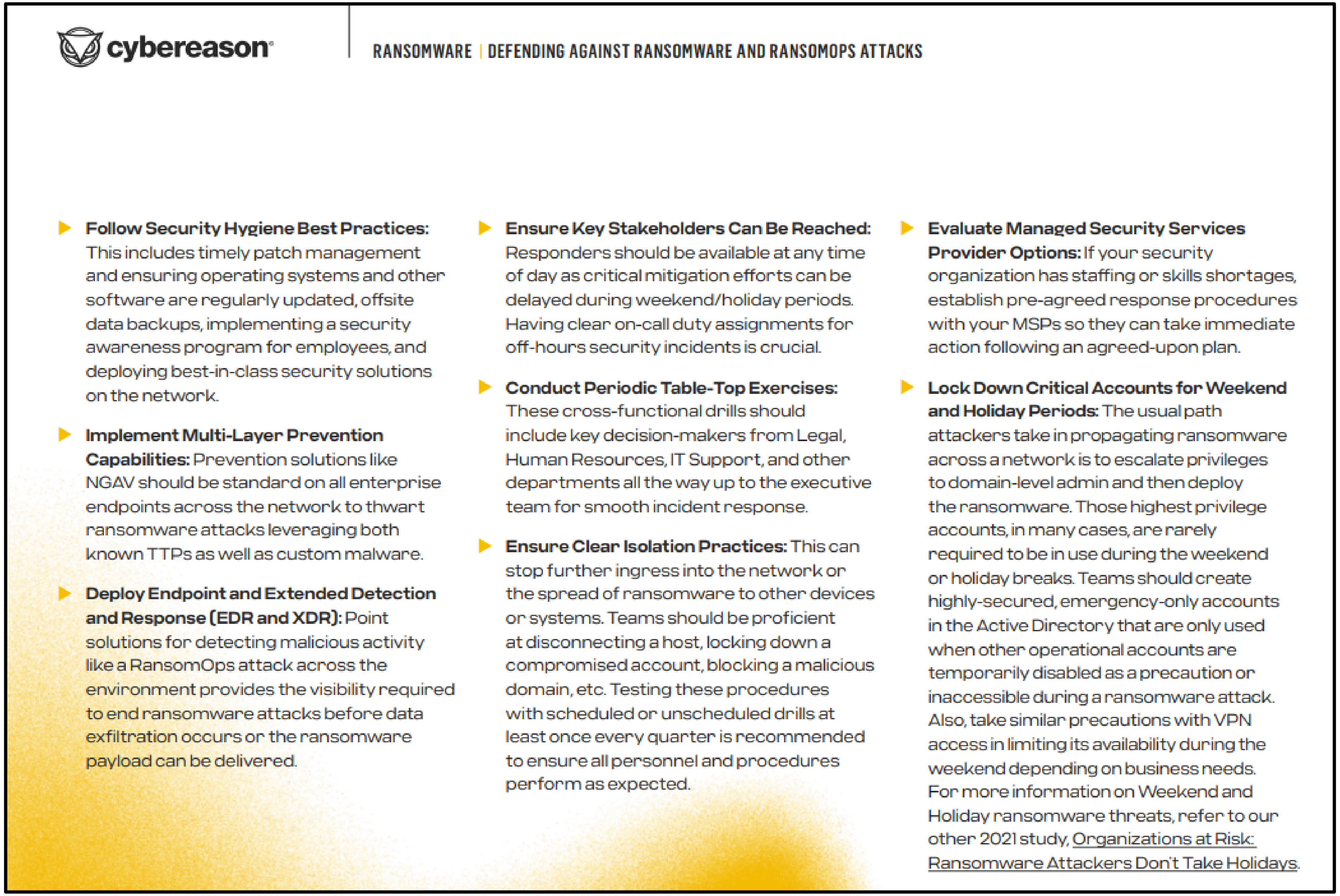
Once an organization has been compromised with ransomware, no clear-cut "best option" is available. If the ransom is not paid, business may grind to a halt for days or weeks as data is manually restored from backups–assuming the organization has backups.

If a ransomware attack includes data exfiltration for double extortion, not paying the ransom also means accepting the risk that sensitive data and intellectual property may be exposed publicly–and the legal and regulatory consequences that can stem from such exposure. Again, the financial, legal, regulatory, and reputational impact of a ransomware attack–including lost business and productivity and the cost of recovery efforts–can often exceed the ransom demand.

The alternative is to pay the ransom, but that comes with issues and risks as well. As noted earlier, many organizations that pay the ransom are able to regain access to their data but find that some or all of it has been corrupted. The decryption tool provided by ransomware attackers is often buggy or slow, forcing companies to restore from their backups even after paying the ransom. There is also no guarantee that your data won't still be sold online after paying the ransom.

The best option for defending against ransomware is to be proactive and prevent an attack at the outset, to detect and disrupt an attack in progress as early as possible, and to be prepared to respond to a successful attack swiftly.

https://www.cybereason.com/ransomware-the-true-cost-to-business-2022?



cybereason

RANSOMWARE | DEFENDING AGAINST RANSOMWARE AND RANSOMOPS ATTACKS

- **Follow Security Hygiene Best Practices:** This includes timely patch management and ensuring operating systems and other software are regularly updated, offsite data backups, implementing a security awareness program for employees, and deploying best-in-class security solutions on the network.
- **Implement Multi-Layer Prevention Capabilities:** Prevention solutions like NGAV should be standard on all enterprise endpoints across the network to thwart ransomware attacks leveraging both known TTPs as well as custom malware.
- **Deploy Endpoint and Extended Detection and Response (EDR and XDR):** Point solutions for detecting malicious activity like a RansomOps attack across the environment provides the visibility required to end ransomware attacks before data exfiltration occurs or the ransomware payload can be delivered.
- **Ensure Key Stakeholders Can Be Reached:** Responders should be available at any time of day as critical mitigation efforts can be delayed during weekend/holiday periods. Having clear on-call duty assignments for off-hours security incidents is crucial.
- **Conduct Periodic Table-Top Exercises:** These cross-functional drills should include key decision-makers from Legal, Human Resources, IT Support, and other departments all the way up to the executive team for smooth incident response.
- **Ensure Clear Isolation Practices:** This can stop further ingress into the network or the spread of ransomware to other devices or systems. Teams should be proficient at disconnecting a host, locking down a compromised account, blocking a malicious domain, etc. Testing these procedures with scheduled or unscheduled drills at least once every quarter is recommended to ensure all personnel and procedures perform as expected.
- **Evaluate Managed Security Services Provider Options:** If your security organization has staffing or skills shortages, establish pre-agreed response procedures with your MSPs so they can take immediate action following an agreed-upon plan.
- **Lock Down Critical Accounts for Weekend and Holiday Periods:** The usual path attackers take in propagating ransomware across a network is to escalate privileges to domain-level admin and then deploy the ransomware. Those highest privilege accounts, in many cases, are rarely required to be in use during the weekend or holiday breaks. Teams should create highly-secured, emergency-only accounts in the Active Directory that are only used when other operational accounts are temporarily disabled as a precaution or inaccessible during a ransomware attack. Also, take similar precautions with VPN access in limiting its availability during the weekend depending on business needs. For more information on Weekend and Holiday ransomware threats, refer to our other 2021 study, Organizations at Risk: Ransomware Attackers Don't Take Holidays.

https://www.cybereason.com/ransomware-the-true-cost-to-business-2022?

Attack Surface

The complexity of information technology is staggering, …
… and we will often need to protect assets like:

Applications:

Languages, Source Code Logic, Domains, URLs, Libraries, Containers, Packet Managers, Databases, Frontend Applications, Native Apps, Backend Applications, APIs, LAMP/SMACK stacks, Files (JPGs, PDFs, etc.)

https://medium.com/the-ciso-den/evidence-based-cybersecurity-management-in-a-nutshell-assets-and-their-stakeholders-4-8-a63c68a92744

Attack Surface

The complexity of information technology is staggering, …
… and we will often need to protect assets like:

Networks:

IP Stack including DHCP, DNS, BGP, IPv6, internal and external IP ranges, Network Stack (e.g. Ethernet), VPN, WiFi, Routers, Switches, APs, Firewall, IDS/IPS, WAF

https://medium.com/the-ciso-den/evidence-based-cybersecurity-management-in-a-nutshell-assets-and-their-stakeholders-4-8-a63c68a92744

Attack Surface

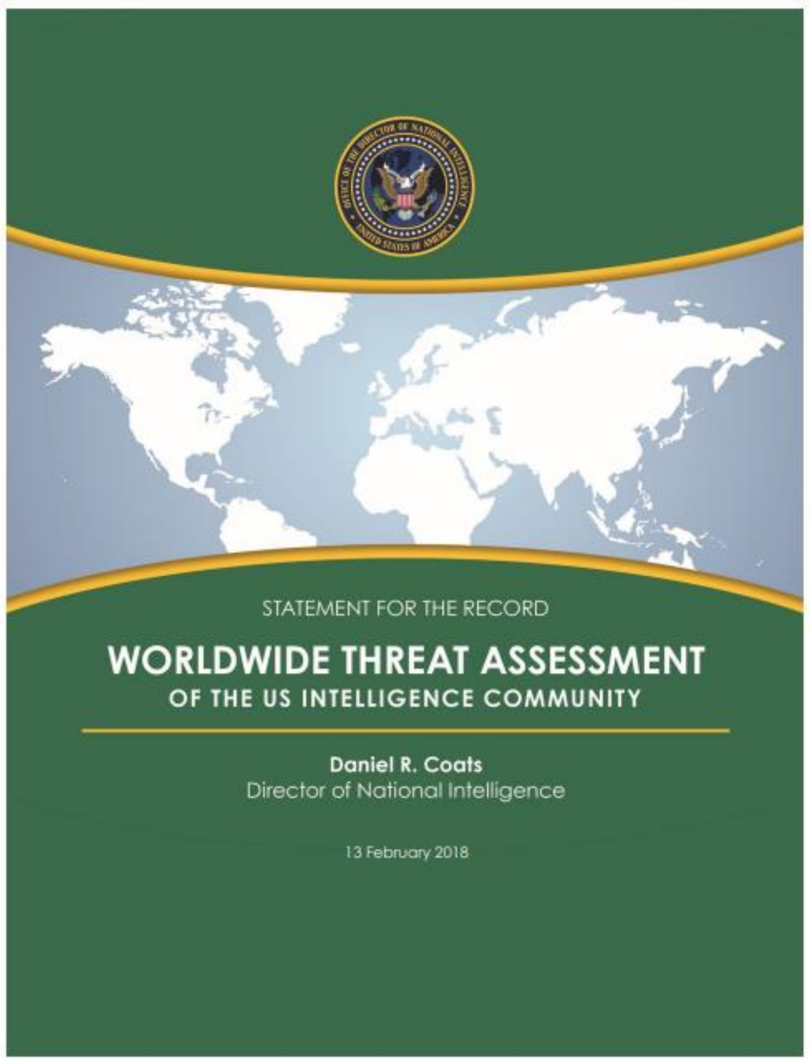
The complexity of information technology is staggering, …
… and we will often need to protect assets like:

Systems:

Operating Systems, Hypervisors, Containers, Orchestration, Cloud Infrastructure Instances, Cloud Storage Services, Directories, Password Managers, Email, Chat, PKIs and Digital Certificates, Anti-Malware solutions, UEFI, Personal computers, Mobile Devices, Servers, SIEM, Encryption and Tokenization, Licenses, Proxy, NTP and Synchronization Services

https://medium.com/the-ciso-den/evidence-based-cybersecurity-management-in-a-nutshell-assets-and-their-stakeholders-4-8-a63c68a92744

DNI 2018 Threat Assessment



STATEMENT FOR THE RECORD

WORLDWIDE THREAT ASSESSMENT
OF THE US INTELLIGENCE COMMUNITY

Daniel R. Coats
Director of National Intelligence

13 February 2018

2018

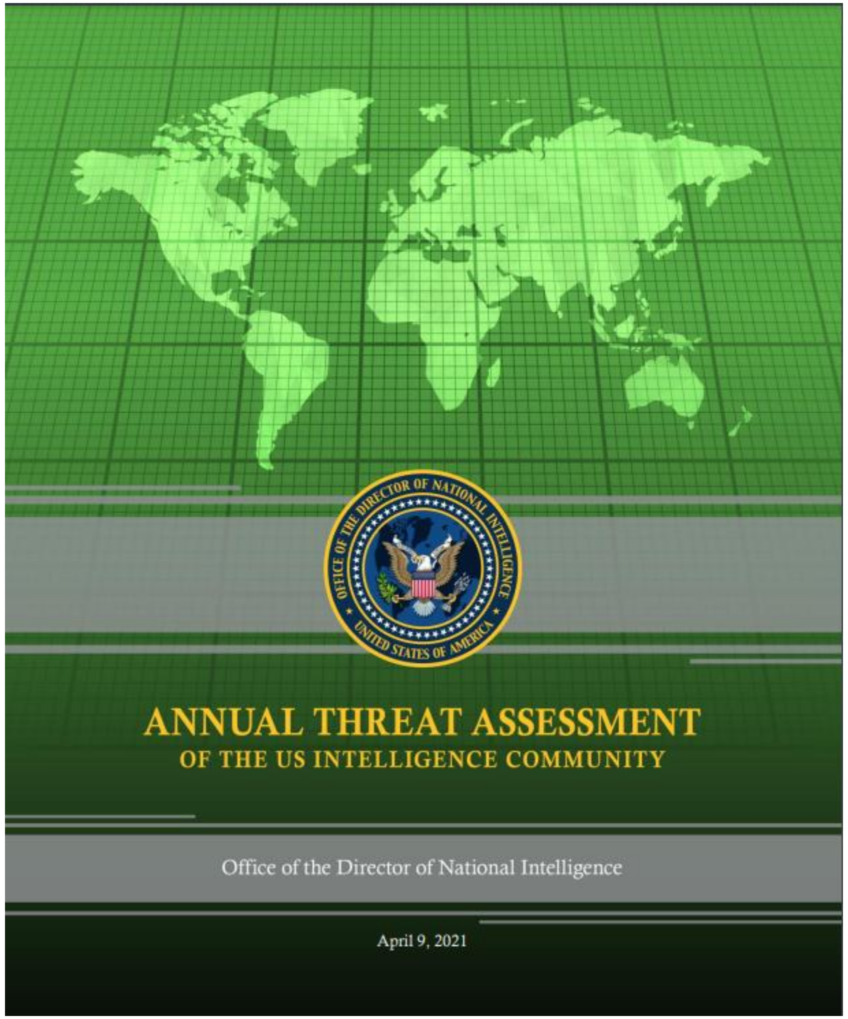
CYBER THREATS

*The potential for surprise in the cyber realm will increase in the next year [**2019**] and beyond as billions more digital devices are connected—with relatively little built-in security—and both nation states and malign actors become more emboldened and better equipped in the use of increasingly widespread cyber toolkits.*

The risk is growing that some adversaries will conduct cyber attacks—such as data deletion or localized and temporary disruptions of critical infrastructure—against the United States in a crisis short of war. …

Ransomware and malware attacks have spread globally, disrupting global shipping and production lines of US companies. The availability of criminal and commercial malware is creating opportunities for new actors to launch cyber operations.

DNI 2021 Threat Assessment



ANNUAL THREAT ASSESSMENT
OF THE US INTELLIGENCE COMMUNITY

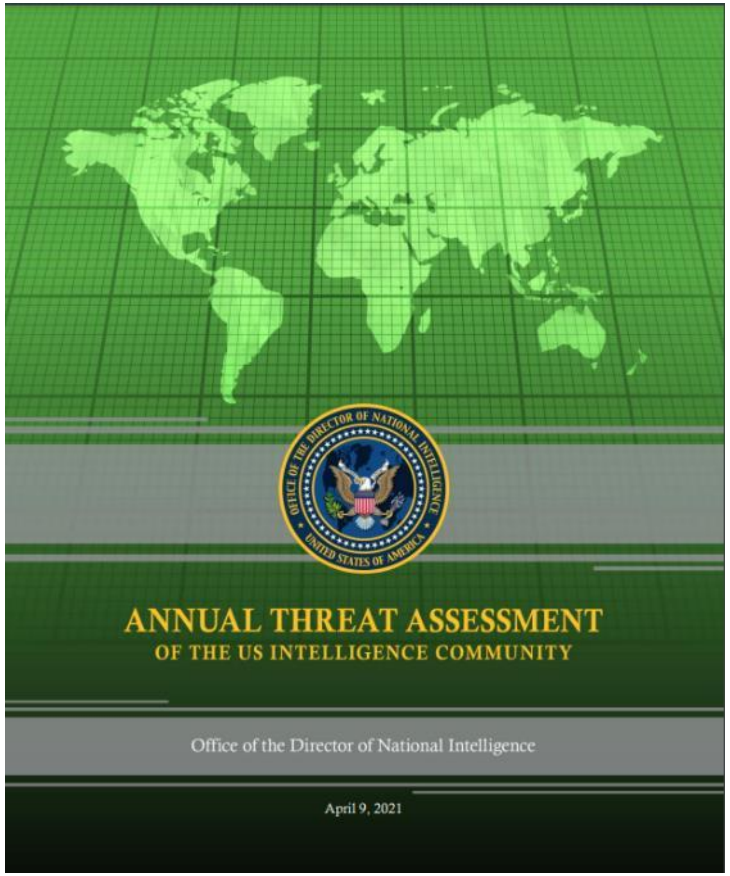
Office of the Director of National Intelligence

April 9, 2021

Cyber threats from nation states and their surrogates will remain acute. *Foreign states use cyber operations to steal information, influence populations, and damage industry, including physical and digital critical infrastructure. … we remain most concerned about Russia, China, Iran, and North Korea.*

Annual Threat Assessment of the US Intelligence Community
Office of the Director of National Intelligence
April 9, 2021

DNI 2021 Threat Assessment



ANNUAL THREAT ASSESSMENT
OF THE US INTELLIGENCE COMMUNITY

Office of the Director of National Intelligence

April 9, 2021

China *almost certainly is capable of launching cyber attacks that would disrupt critical infrastructure services within the United States, including against oil and gas pipelines and rail systems. …*

Russia *is particularly focused on improving its ability to target critical infrastructure, including underwater cables and industrial control systems …*

Iran*'s growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of U.S. and allied networks and data.*

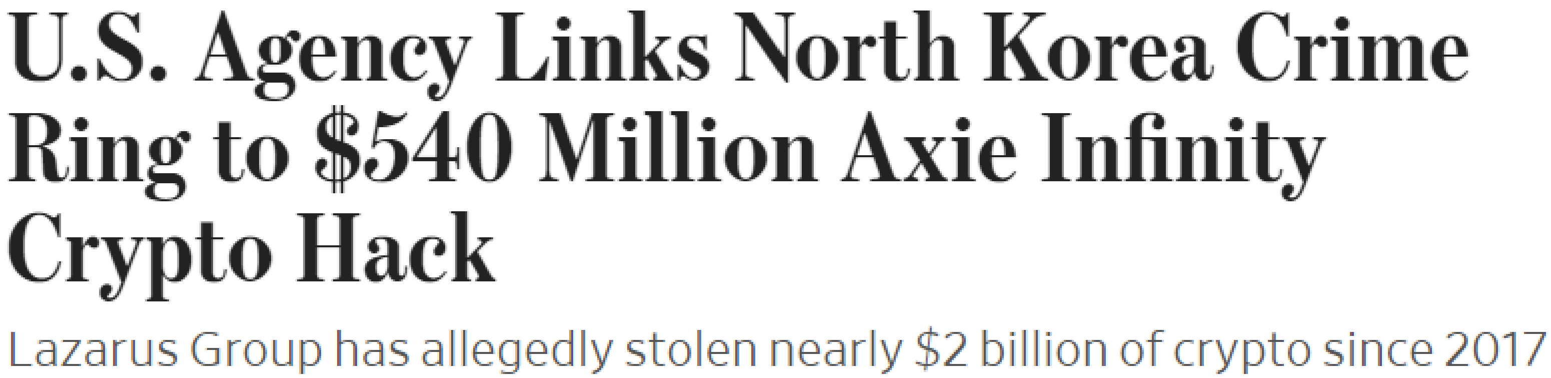
Cyber actors linked to **North Korea** *have conducted espionage efforts against a range of organizations, including media, academia, defense companies, and governments, in multiple countries.*

Transnational cyber criminals *are increasing the number, scale, and sophistication of ransomware attacks, fueling a virtual ecosystem that threatens to cause greater disruptions of critical services worldwide. …*

… Attackers are innovating their targeting strategies to focus on victims whose business operations lack resilience or whose consumer base cannot sustain service disruptions, driving ransomware payouts up.

4/14/2022

THE WALL STREET JOURNAL.

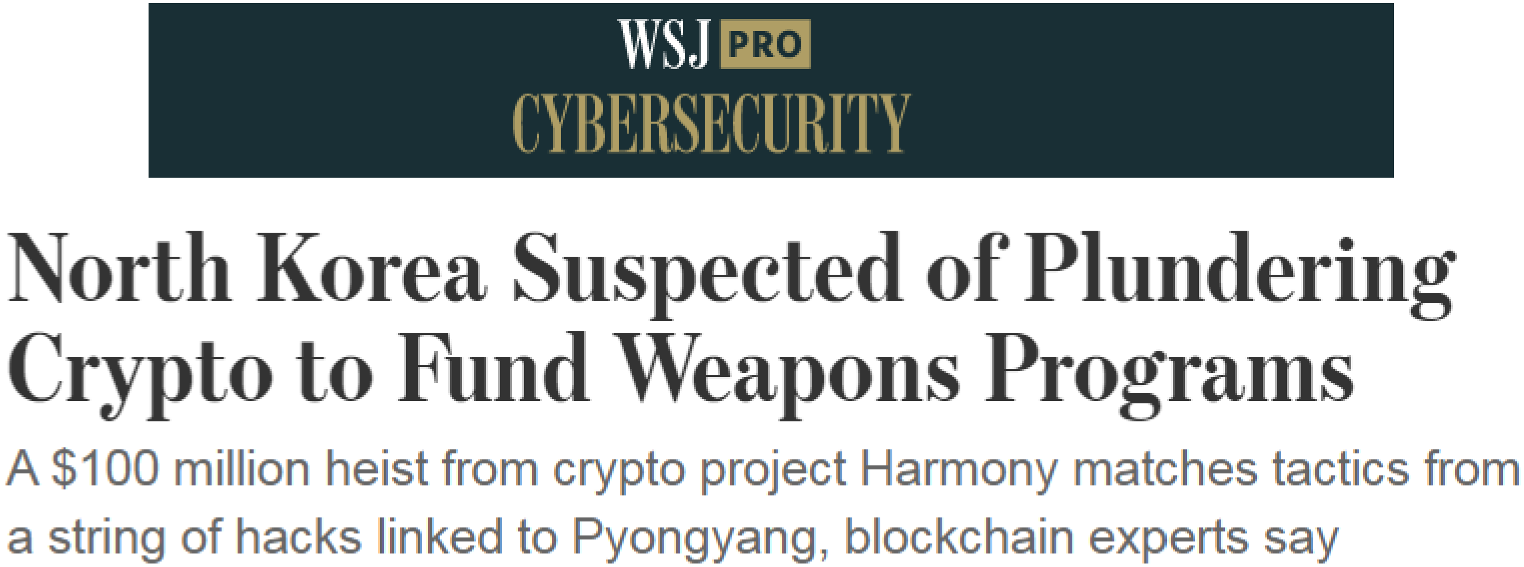


U.S. Agency Links North Korea Crime Ring to $540 Million Axie Infinity Crypto Hack

Lazarus Group has allegedly stolen nearly $2 billion of crypto since 2017

https://www.wsj.com/articles/u-s-agency-links-north-korea-crime-ring-to-540-million-axie-infinity-crypto-hack-11649966631

7/1/2022



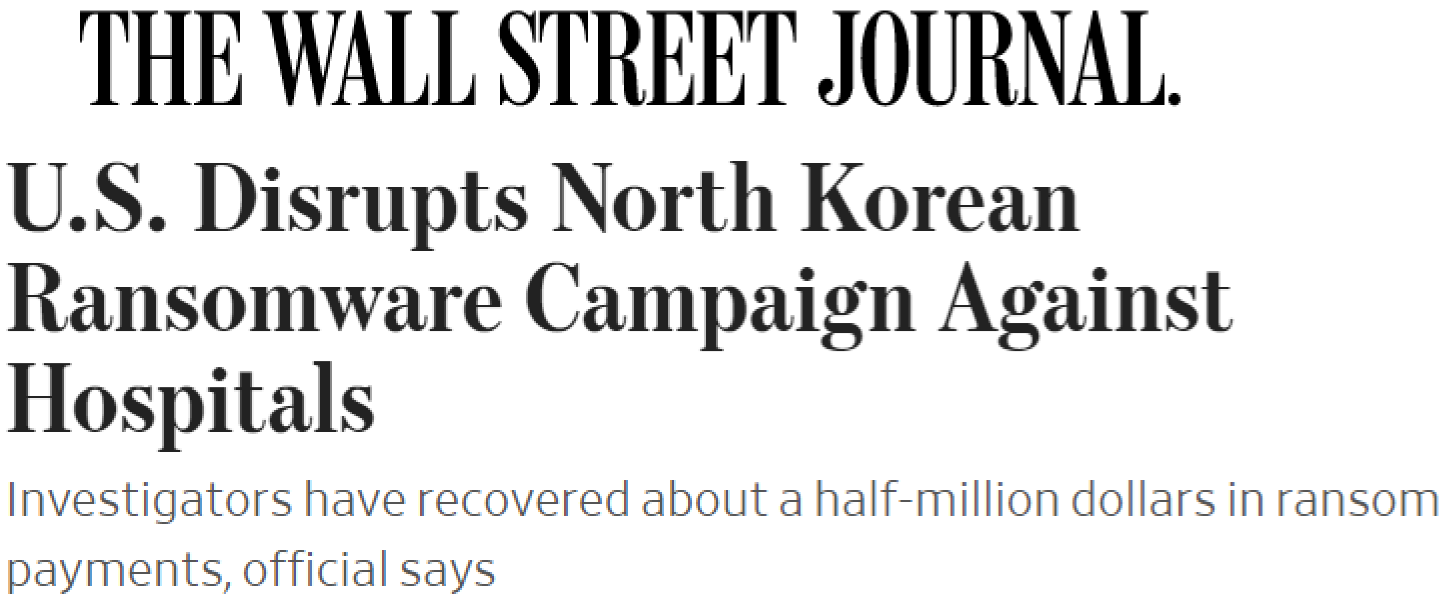
WSJ PRO CYBERSECURITY

North Korea Suspected of Plundering Crypto to Fund Weapons Programs

A $100 million heist from crypto project Harmony matches tactics from a string of hacks linked to Pyongyang, blockchain experts say

https://www.wsj.com/articles/north-korea-suspected-of-plundering-crypto-to-fund-weapons-programs-11656667802

7/19/2022

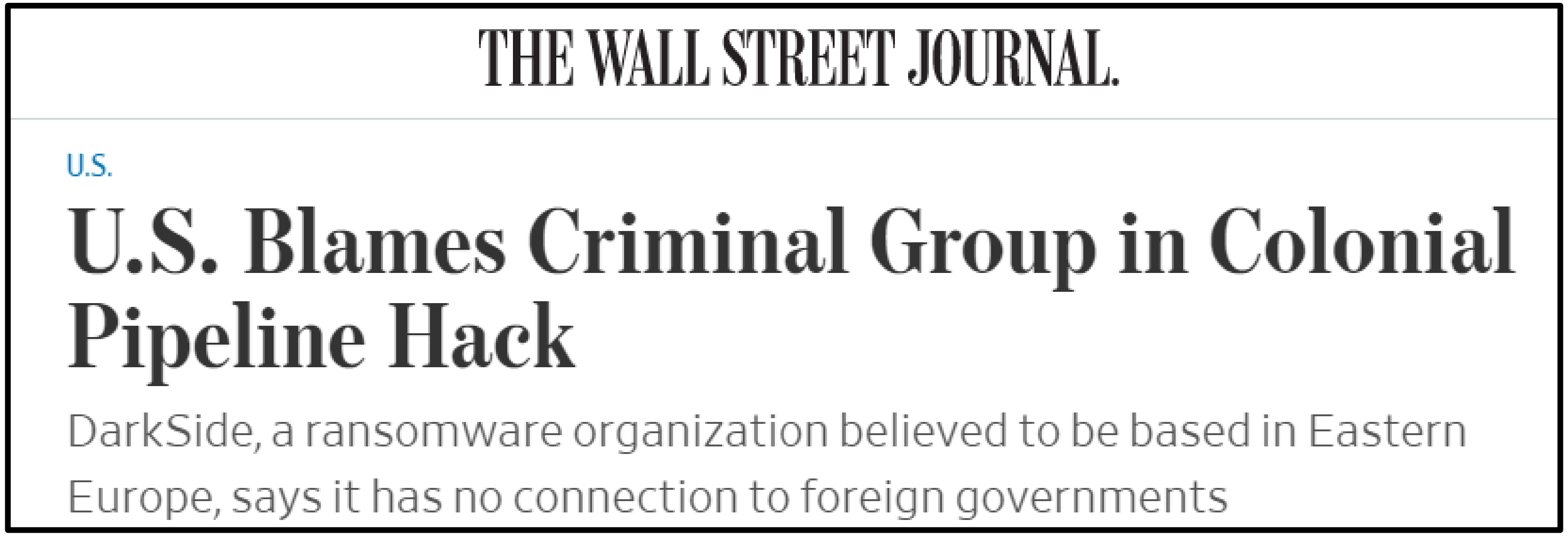


THE WALL STREET JOURNAL.

U.S. Disrupts North Korean Ransomware Campaign Against Hospitals

Investigators have recovered about a half-million dollars in ransom payments, official says

5/10/2021



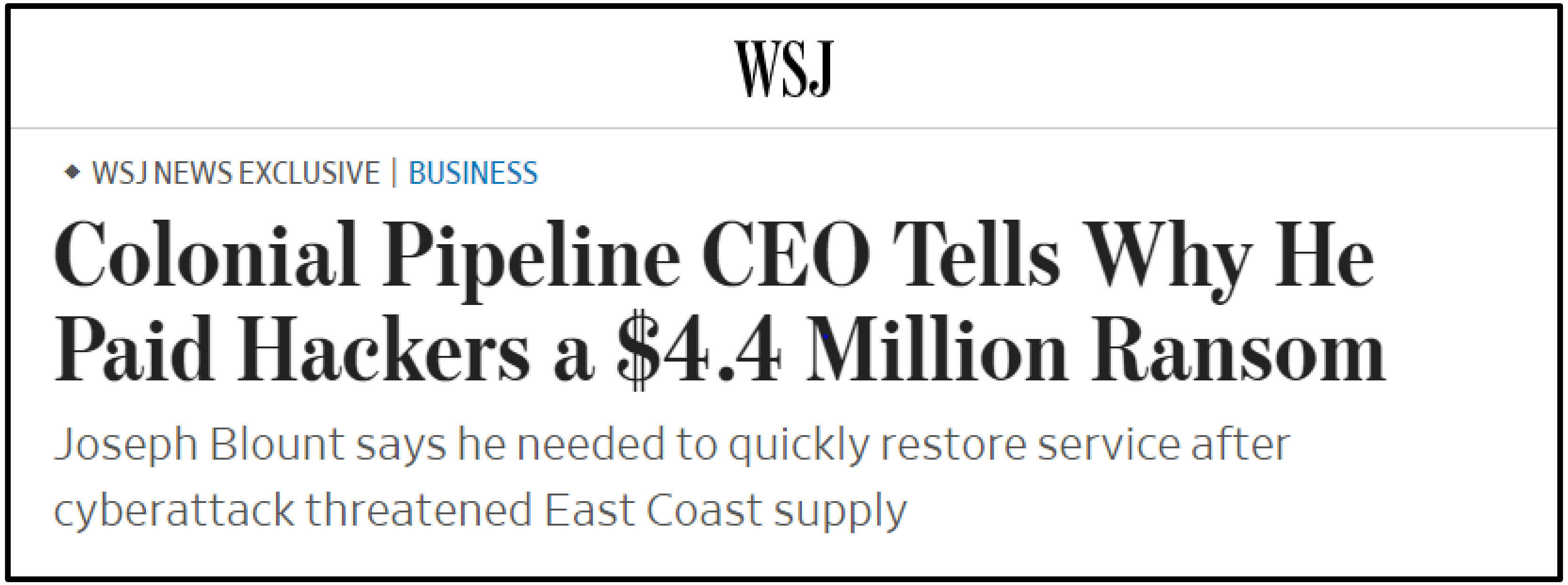
THE WALL STREET JOURNAL.

U.S.

U.S. Blames Criminal Group in Colonial Pipeline Hack

DarkSide, a ransomware organization believed to be based in Eastern Europe, says it has no connection to foreign governments

5/19/2021



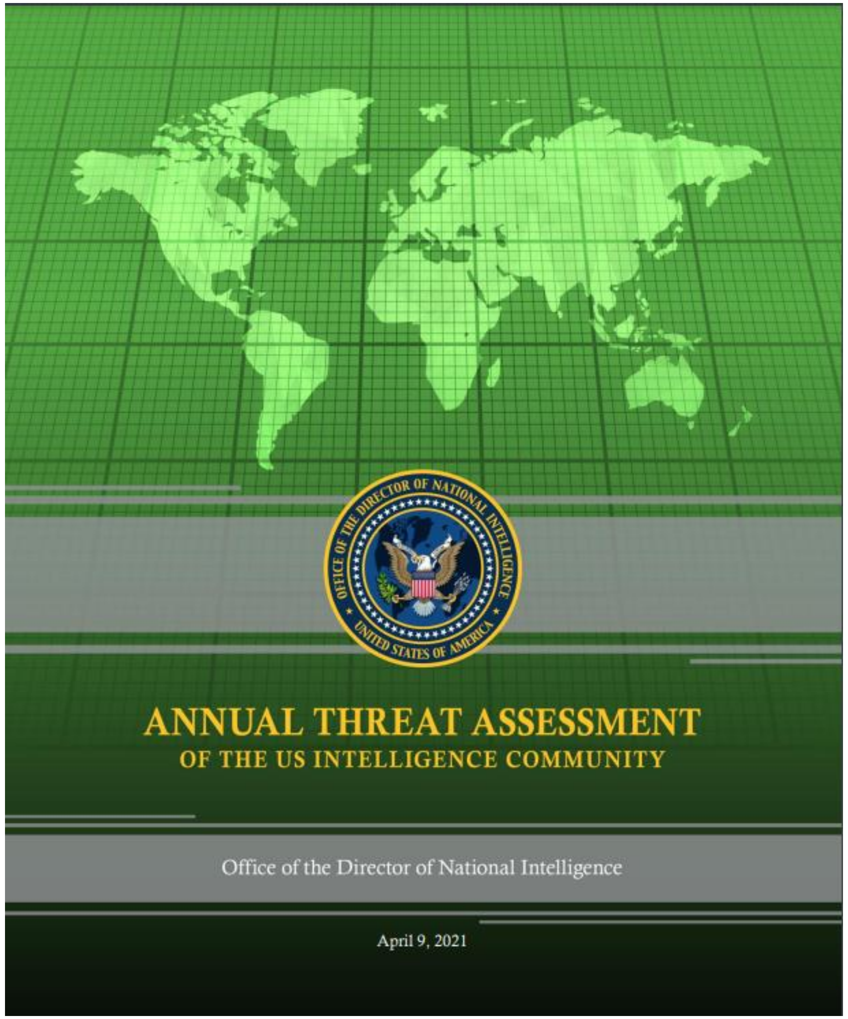
WSJ

◆ WSJ NEWS EXCLUSIVE | BUSINESS

Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom

Joseph Blount says he needed to quickly restore service after cyberattack threatened East Coast supply

DNI 2021 Threat Assessment



ANNUAL THREAT ASSESSMENT
OF THE US INTELLIGENCE COMMUNITY

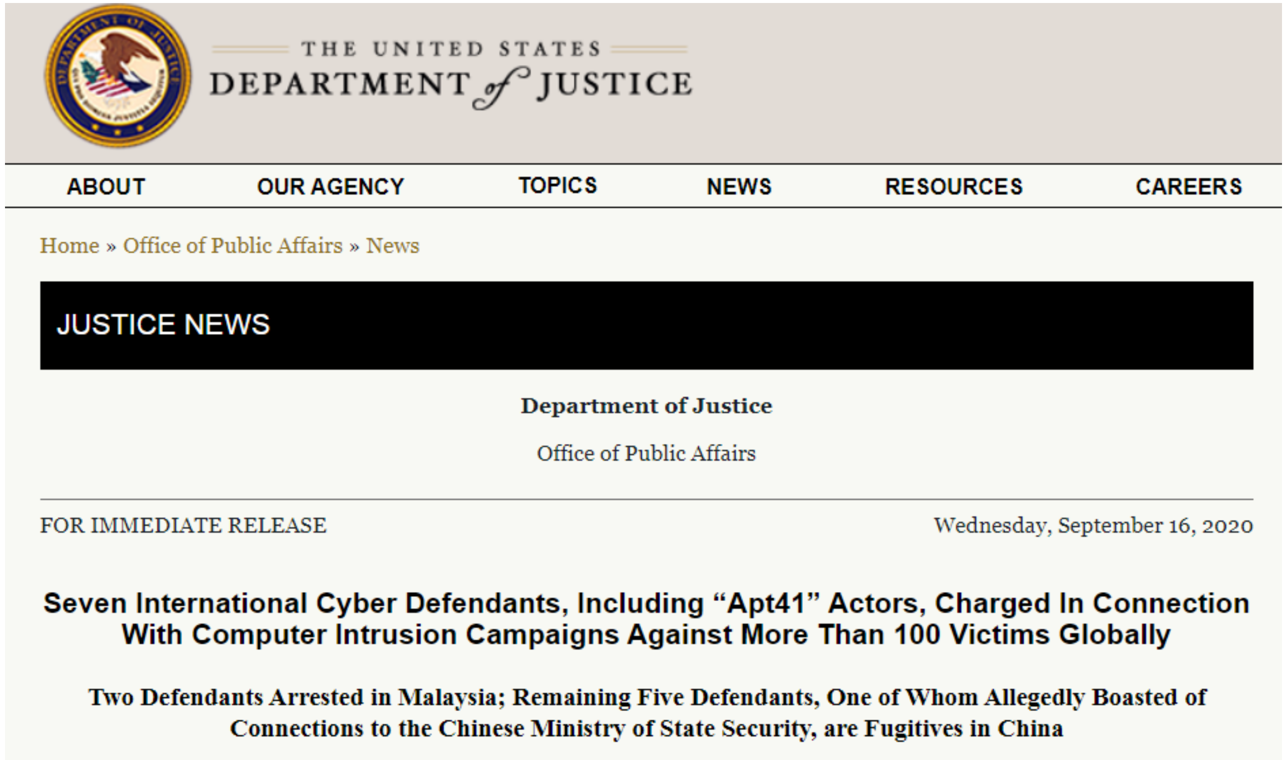
Office of the Director of National Intelligence

April 9, 2021

Cyber threats from nation states and their surrogates will remain acute*. Foreign states use cyber operations to steal information, influence populations, and damage industry, including physical and digital critical infrastructure. … we remain most concerned about Russia, China, Iran, and North Korea.*

Annual Threat Assessment of the US Intelligence Community
Office of the Director of National Intelligence
April 9, 2021

People's Republic of China (PRC) Indictments



Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE Wednesday, September 16, 2020

Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally

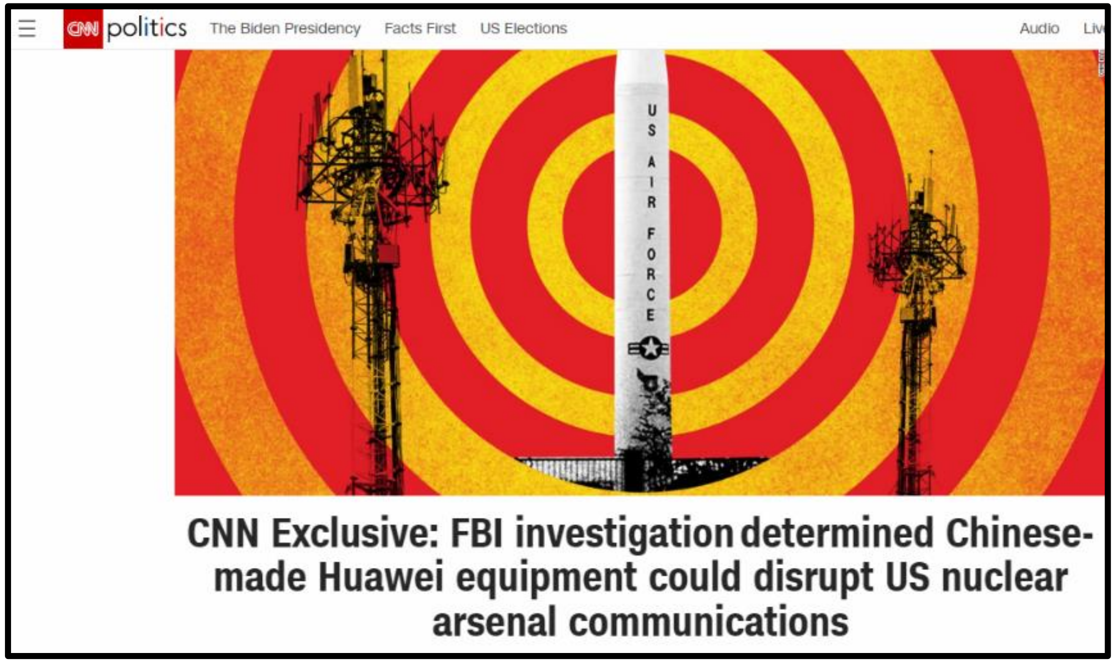
Two Defendants Arrested in Malaysia; Remaining Five Defendants, One of Whom Allegedly Boasted of Connections to the Chinese Ministry of State Security, are Fugitives in China

https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer

The intrusions, which security researchers have tracked using the threat labels "APT41," "Barium," "Winnti," "Wicked Panda," and "Wicked Spider," facilitated the theft of source code, software code signing certificates, customer account data, and valuable business information.

These intrusions also facilitated the defendants' other criminal schemes, including ransomware and "crypto-jacking" schemes, the latter of which refers to the group's unauthorized use of victim computers to "mine" cryptocurrency.

China (Yet Again)



CNN Exclusive: FBI investigation determined Chinese-made Huawei equipment could disrupt US nuclear arsenal communications

https://www.cnn.com/2022/07/23/politics/fbi-investigation-huawei-china-defense-department-communications-nuclear/index.html

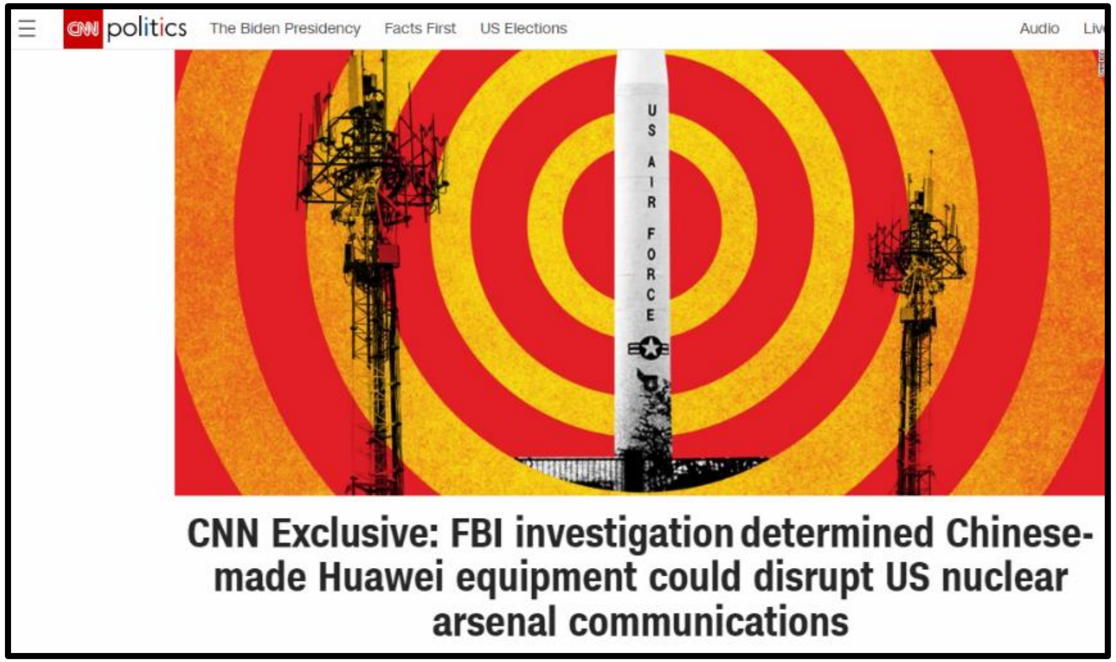
Updated 12:01 AM ET, Sat July 23, 2022

In 2017, the Chinese government was offering to spend $100 million to build an ornate Chinese garden at the National Arboretum in Washington DC. Complete with temples, pavilions and a 70-foot white pagoda …

… strategically placed on one of the highest points in Washington DC, just two miles from the US Capitol, a perfect spot for signals intelligence collection …

… wanted to build the pagoda with materials shipped to the US in diplomatic pouches, which US Customs officials are barred from examining, the sources said.

China (Yet Again)



CNN Exclusive: FBI investigation determined Chinese-made Huawei equipment could disrupt US nuclear arsenal communications

https://www.cnn.com/2022/07/23/politics/fbi-investigation-huawei-china-defense-department-communications-nuclear/index.html

Updated 12:01 AM ET, Sat July 23, 2022

Chinese-made Huawei equipment atop cell towers near US military bases in the rural Midwest. According to multiple sources familiar with the matter, the FBI determined the equipment was capable of capturing and disrupting highly restricted Defense Department communications, including those used by US Strategic Command, which oversees the country's nuclear weapons. …

… no question the Huawei equipment has the ability to intercept not only commercial cell traffic but also the highly restricted airwaves used by the military and disrupt critical US Strategic Command communications, giving the Chinese government a potential window into America's nuclear arsenal.

China (Yet Again)

CYBER SAFETY REVIEW BOARD

Review of the December 2021 Log4j Event

Publication: July 11, 2022
Cyber Safety Review Board

July 11, 2022

… The requirement for network product providers to report vulnerabilities in their products to MIIT [China's Ministry of Industry and Information] *within two days of discovery could give the PRC government early knowledge of vulnerabilities before vendor fixes are made available to the community.*

The Board is concerned this will afford the PRC government a window in which to exploit vulnerabilities before network defenders can patch them.

This is a disturbing prospect given the PRC government's known track record of intellectual property theft,[135] intelligence collection,[136] surveillance of human rights activists and dissidents,[137] and military cyber operations.[138] …

[135] Financial Times, "America is struggling to counter China's intellectual property theft," April 18, 2022, https://www.ft.com/content/1d13ab71-bffd-4d63-a0bf-9e9bdfc33c39

[136] Cheng, Dean, The Heritage Foundation, Congressional Testimony, "The PRC and Intelligence Gathering: Unconventional Targets and Unconventional Methods," December 12, 2018, https://www.judiciary.senate.gov/download/12-12-18-cheng-testimony

[137] Freedom House, "China: Transnational Repression Case Study," February 2021, https://freedomhouse.org/report/transnational-repression/china

[138] Cybersecurity and Infrastructure Security Agency (CISA), "Alert (AA21-200B) Chinese State-Sponsored Cyber Operations: Observed TTPs," July 19, 2021, https://www.cisa.gov/uscert/ncas/alerts/aa21-200b

China (Yet Again)

Andrea Peterson | July 19, 2022

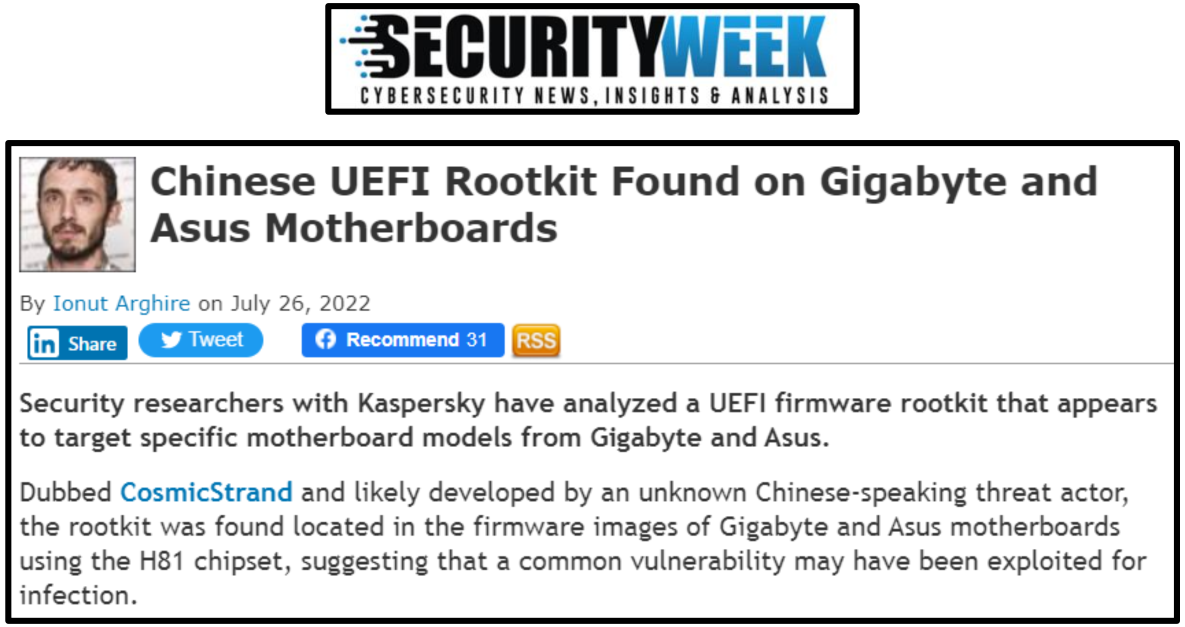
Unpatched flaws in popular GPS devices could let hackers disrupt and track vehicles

BitSight reported it discovered six flaws in the **Chinese** supplier MiCODUS's MV720 device, which is designed to be hardwired into vehicles. According to advertisements on MiCODUS's web site, the device allows vehicles to be tracked in real-time via text messaging and an app. It also includes a remote shutdown capability that relies on disabling the vehicle's fuel circuit.

The flaws disclosed by BitSight and CISA include authentication issues that could allow such features to be hijacked — potentially putting drivers in danger and disrupting supply chains.

https://therecord.media/unpatched-flaws-in-popular-gps-devices-could-let-hackers-disrupt-and-track-vehicles/

China (Yet Again)



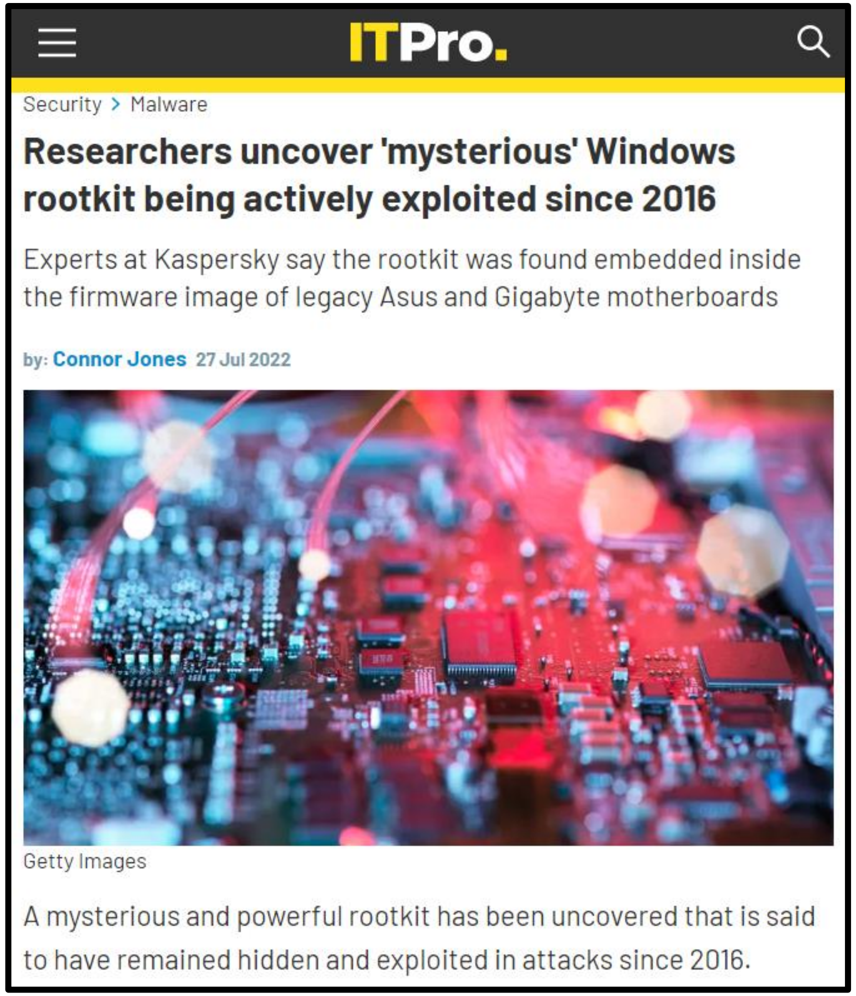
Chinese UEFI Rootkit Found on Gigabyte and Asus Motherboards

By Ionut Arghire on July 26, 2022

Security researchers with Kaspersky have analyzed a UEFI firmware rootkit that appears to target specific motherboard models from Gigabyte and Asus.

Dubbed CosmicStrand and likely developed by an unknown Chinese-speaking threat actor, the rootkit was found located in the firmware images of Gigabyte and Asus motherboards using the H81 chipset, suggesting that a common vulnerability may have been exploited for infection.

https://www.securityweek.com/chinese-uefi-rootkit-found-gigabyte-and-asus-motherboards



Researchers uncover 'mysterious' Windows rootkit being actively exploited since 2016

Experts at Kaspersky say the rootkit was found embedded inside the firmware image of legacy Asus and Gigabyte motherboards

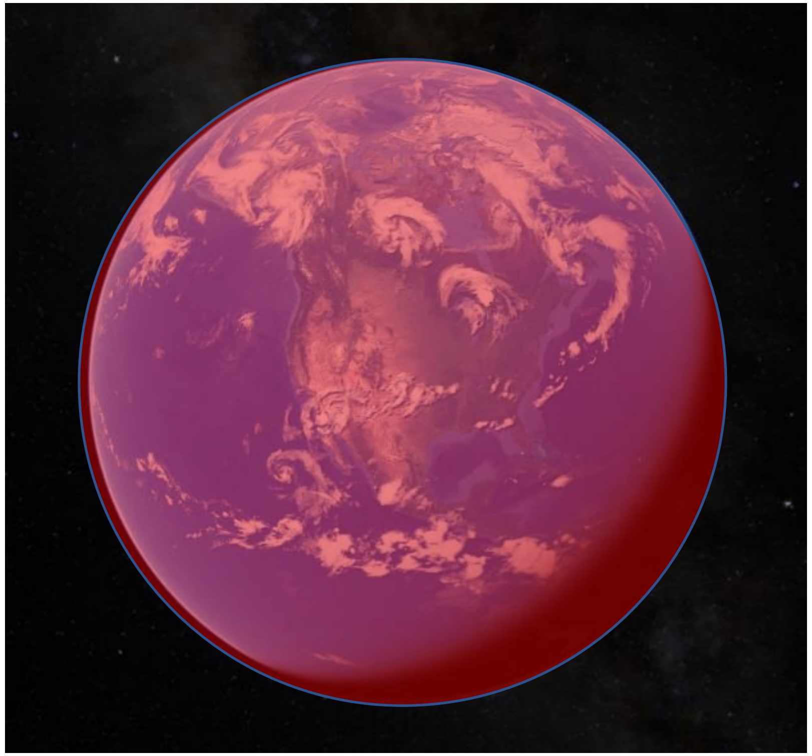
by: Connor Jones 27 Jul 2022

Getty Images

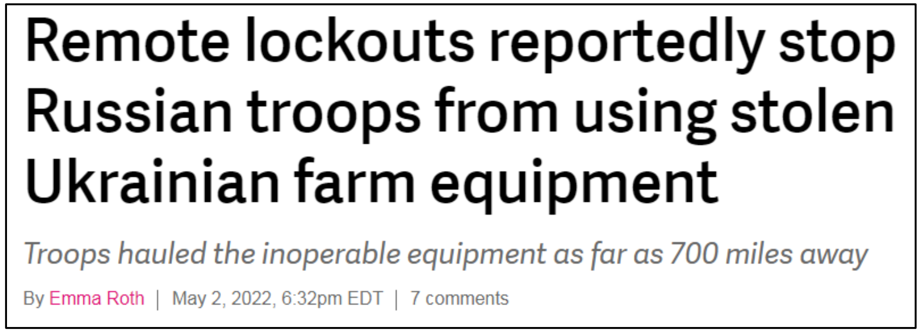
A mysterious and powerful rootkit has been uncovered that is said to have remained hidden and exploited in attacks since 2016.

https://www.itpro.com/security/malware/368655/researchers-uncover-mysterious-windows-rootkit-actively-exploited-2016

China (Yet Again)



North America Geofence



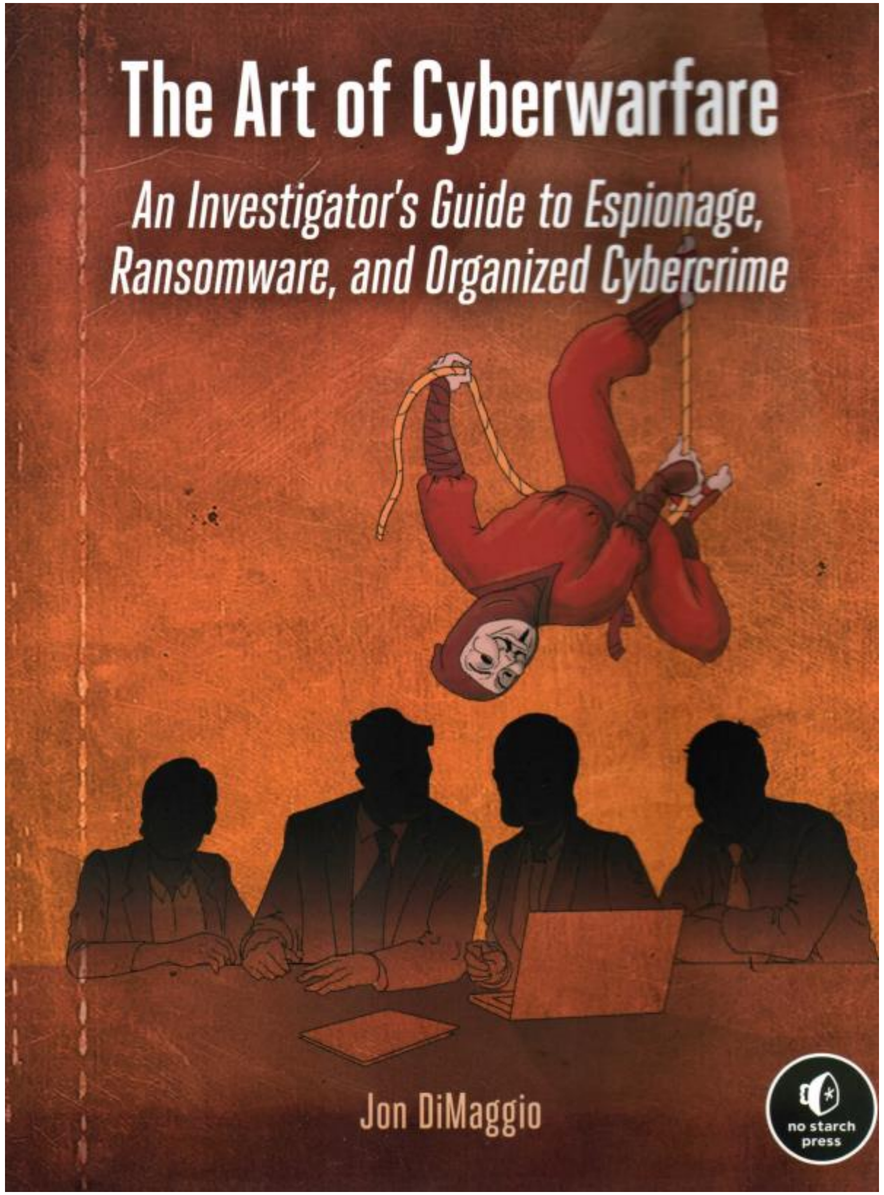
Remote lockouts reportedly stop Russian troops from using stolen Ukrainian farm equipment

Troops hauled the inoperable equipment as far as 700 miles away

By Emma Roth | May 2, 2022, 6:32pm EDT | 7 comments

https://www.theverge.com/2022/5/2/23053944/russian-troops-steal-millions-farm-equipment-ukraine-disabled-remotely-john-deere

China (Yet Again)

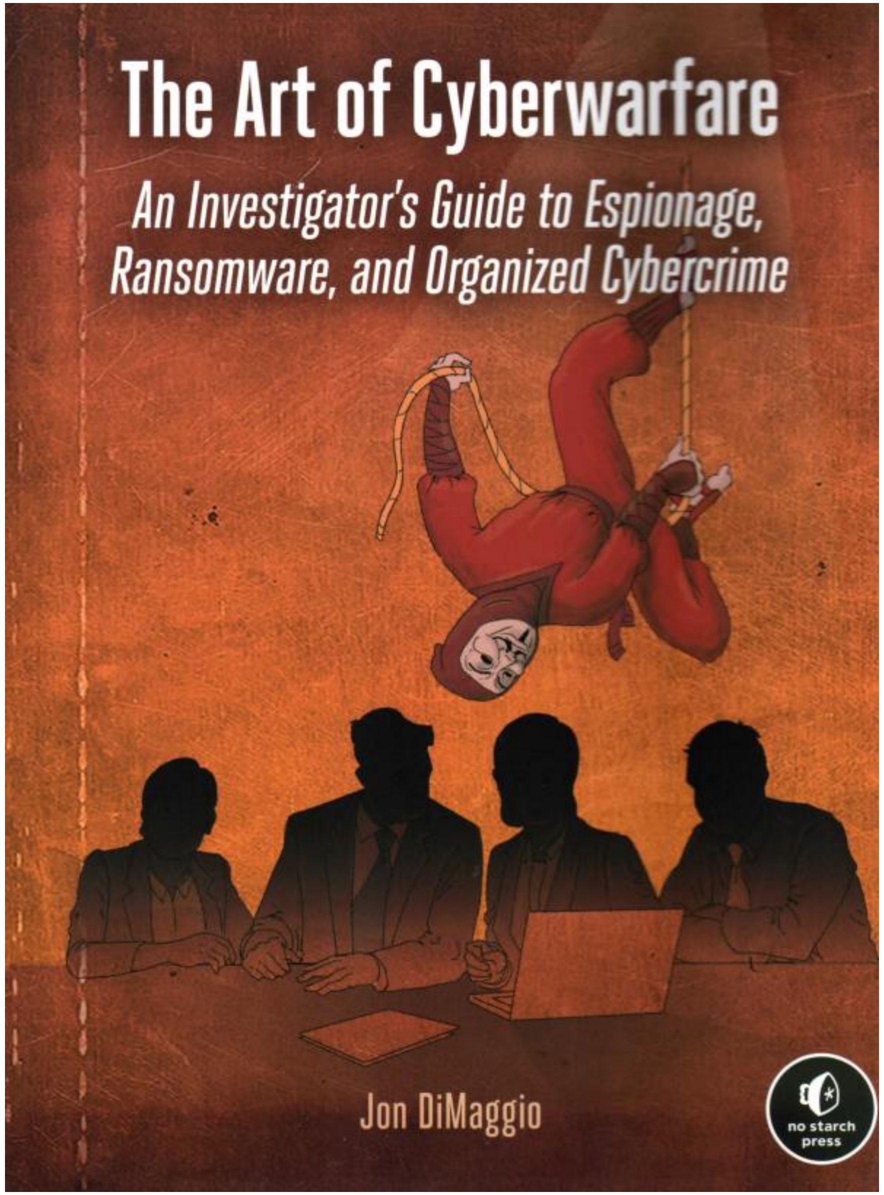

The Art of Cyberwarfare
An Investigator's Guide to Espionage, Ransomware, and Organized Cybercrime
Jon DiMaggio
no starch press

In 1975, Ye Jianying, one of the founders of the People's Liberation Army (PLA), presented a report to the Central Committee of the Communist Party of Chin titled "Strengthening Electronic Countermeasure Work."

The country hoped to surpass the United States as the world's largest superpower by 2049, which marks he 100th anniversary of the founding of the People's Republic of China.

Ye's report showed how China could use electronic warfare as a weapon to strengthen its military force and increase its position as a world power.

China (Yet Again)


The Art of Cyberwarfare
An Investigator's Guide to Espionage, Ransomware, and Organized Cybercrime
Jon DiMaggio
no starch press

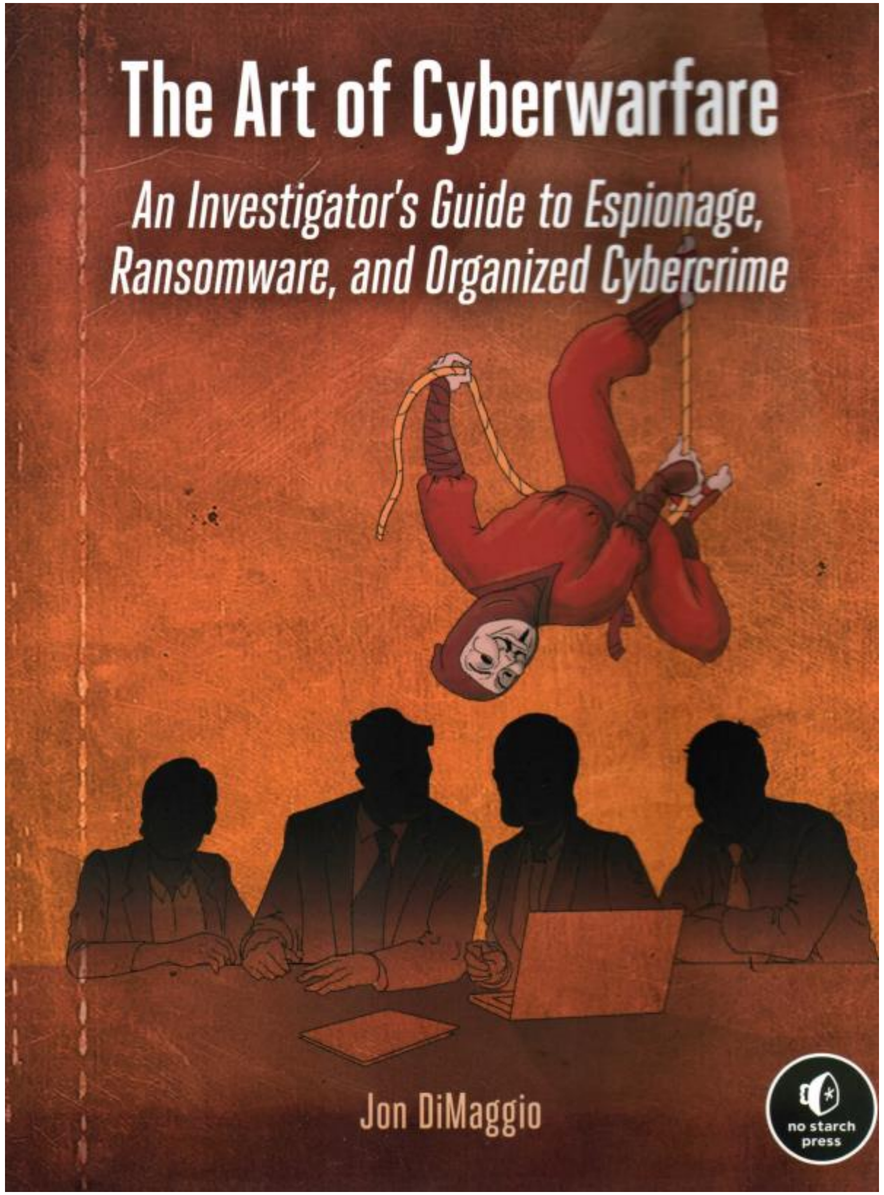
The government soon followed his advice, establishing training programs dedicated to cyberwarfare.

In 1979 it established founded the People's Liberation Army Electronic Engineering College …

… This academic program taught soldiers about the use of computers and networks, focusing on concepts, such as offensive computer operations, that remain relevant to cyberwarfare today.

$$\begin{array}{r} 2022 \\ -\ \underline{1979} \\ 43\ \text{Years} \end{array}$$

China (Yet Again)


The Art of Cyberwarfare
An Investigator's Guide to Espionage, Ransomware, and Organized Cybercrime
Jon DiMaggio
no starch press

Based on publicly available information, it appears China has ben executing cyberwarfare operations since at least 2003, largely motivated by intellectual property theft.

2022
- 2003
19 Years

Transnational Cyber Criminals

THE WALL STREET JOURNAL.

7/19/2022

BUSINESS

The Ruthless Hackers Behind Ransomware Attacks on U.S. Hospitals: 'They Do Not Care'

An Eastern European group known as Ryuk has hit at least 235 facilities, raking in more than $100 million

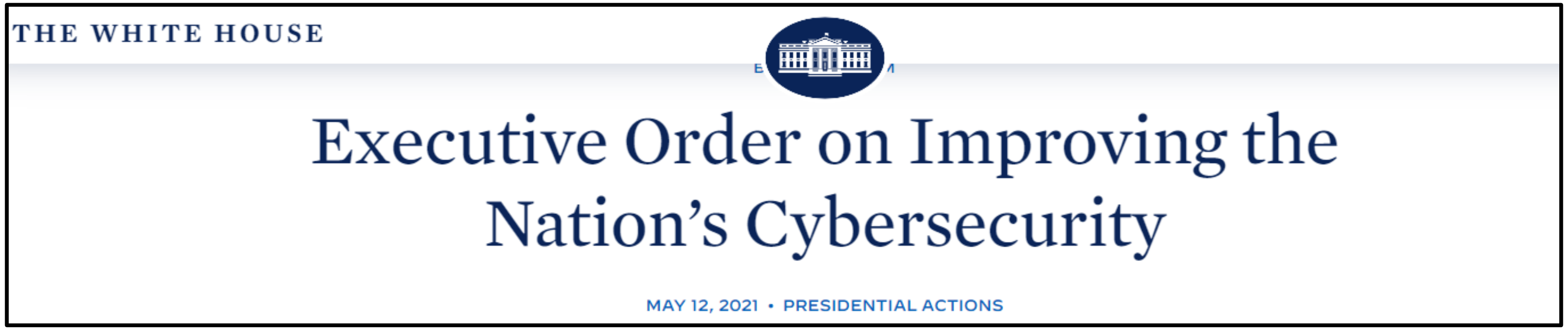
… Ryuk … a notorious gang of Eastern European cybercriminals … with ties to Russian government security services ...

the most prolific ransomware gang in the world, accounting for one-third of the 203 million U.S. ransomware attacks in 2020 … collected at least $100 million in paid ransom last year … targets large organizations with deep resources … routinely extracts six- and seven-figure payments from victims … has hit at least 235 general hospitals and inpatient psychiatric facilities, plus dozens of other healthcare facilities in the U.S. since 2018 …

Hospitals are especially lucrative targets because many have lax cybersecurity controls, and the business of life and death is highly vulnerable to extortion.

Some ransomware gangs avoid them over fears of killing people … Not so with Ryuk.

5/1/2021



THE WHITE HOUSE

Executive Order on Improving the Nation’s Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

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.

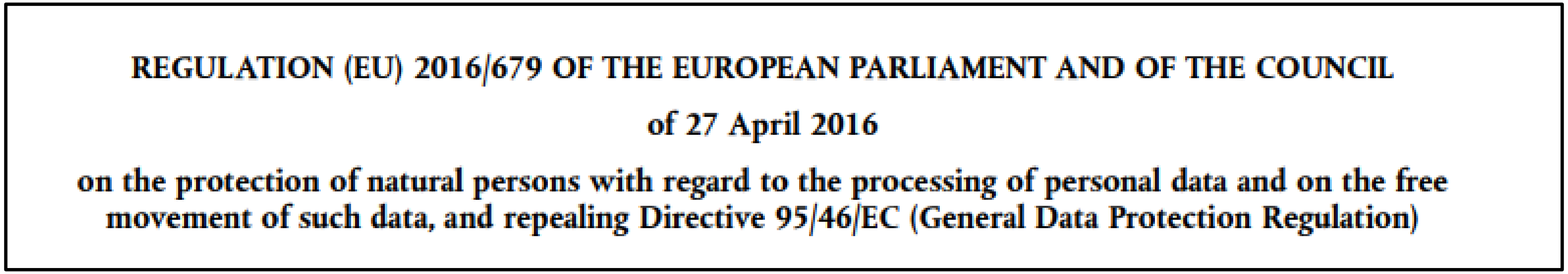
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Breach Notification Overview

When a Breach Occurs, the Problems have Only Started.

EU: The General Data Protection Regulation (GDPR) supervisory authority specifically receives and regulates data protection breach notifications. Data incidents often trigger audits or company reviews.

General Data Protection Regulation (GDPR)



REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 April 2016

on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Breach Notification Overview

When a Breach Occurs, the Problems have Only Started.

U.S.: Each state has data breach notification laws. State attorney generals enforce the patchwork laws, not a data-protection focused regulator that conducts data protection audits.

Notify Which U.S. State Authorities?

Example – *California SB 327*

SB 327, Jackson. Information privacy: connected devices.

Existing law requires a business to take all reasonable steps to dispose of customer records within its custody or control containing personal information when the records are no longer to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable.

Existing law also requires a business that owns, licenses, or maintains personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

all reasonable steps?

reasonable security procedures and practices?

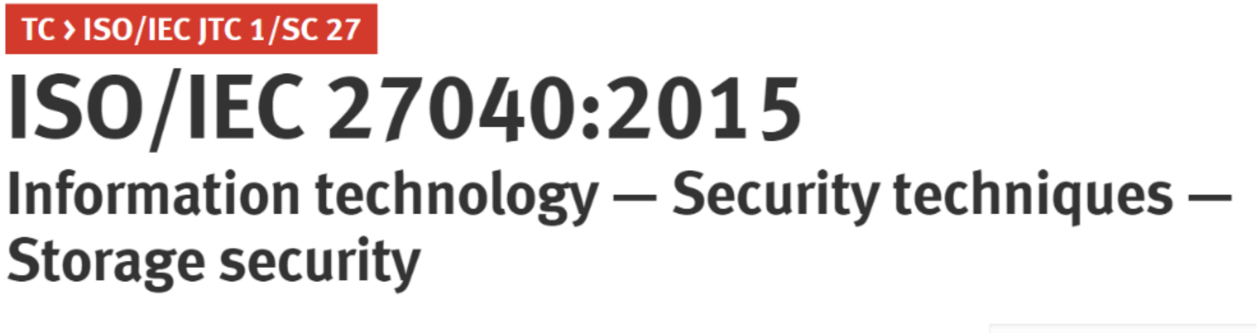
Example – *California SB 327*

SB 327, Jackson. Information privacy: connected devices.

This bill … would require a manufacturer of a [IoT] *connected device … to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure, as specified.*

(b) "Connected device" means any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address.

Legal Exposures - ***Standards***



TC › ISO/IEC JTC 1/SC 27

ISO/IEC 27040:2015

Information technology — Security techniques — Storage security

ISO/IEC 27040:2015 provides detailed technical guidance on how organizations can define an appropriate level of risk mitigation by employing a well-proven and consistent approach to the planning, design, documentation, and implementation of data storage security. Storage security applies to the protection (security) of information where it is stored and to the security of the information being transferred across the communication links associated with storage. Storage security includes the security of devices and media, the security of management activities related to the devices and media, the security of applications and services, and security relevant to end-users during the lifetime of devices and media and after end of use.

International Standard ISO/IEC 27040 ***5.4.1***

Threats for storage systems and infrastructure include, but are not limited to:

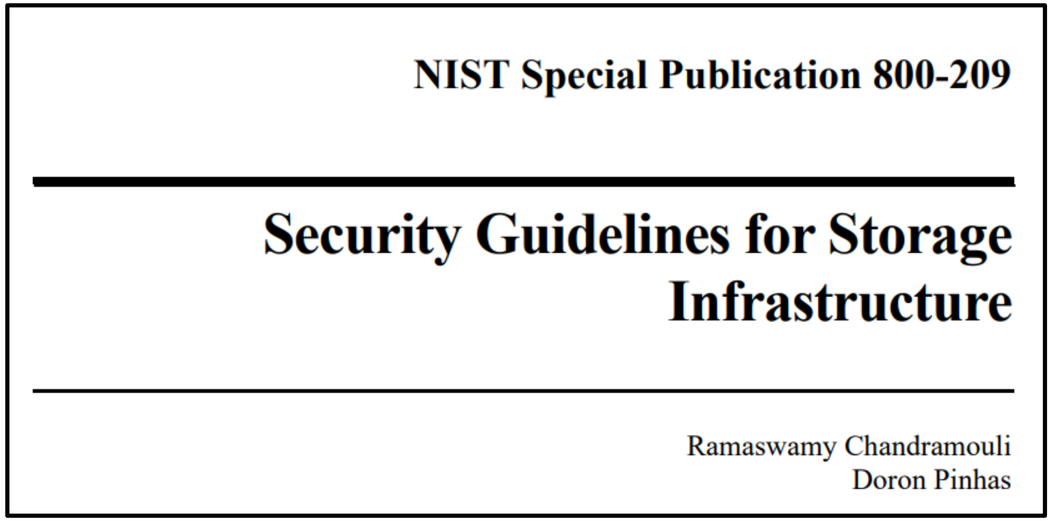
- *unauthorized usage;*
- *unauthorized access;*
- *liability due to regulatory non-compliance;*
- *Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks on storage;*
- *corruption/modification and destruction of data;*
- *data leakage/breaches;*
- *theft or accidental loss of media;*
- *malware attack or introduction;*
- *improper treatment or sanitization after end-of-use.*

… for storage systems and infrastructure the risks associated with data breaches, data corruption or destruction, temporary or permanent loss of access/availability, and failure to meet statutory, regulatory, or legal requirements are the major concerns.

First Edition, 2015-01-15
Pgs. 14-15

Legal Exposures - *Frameworks*

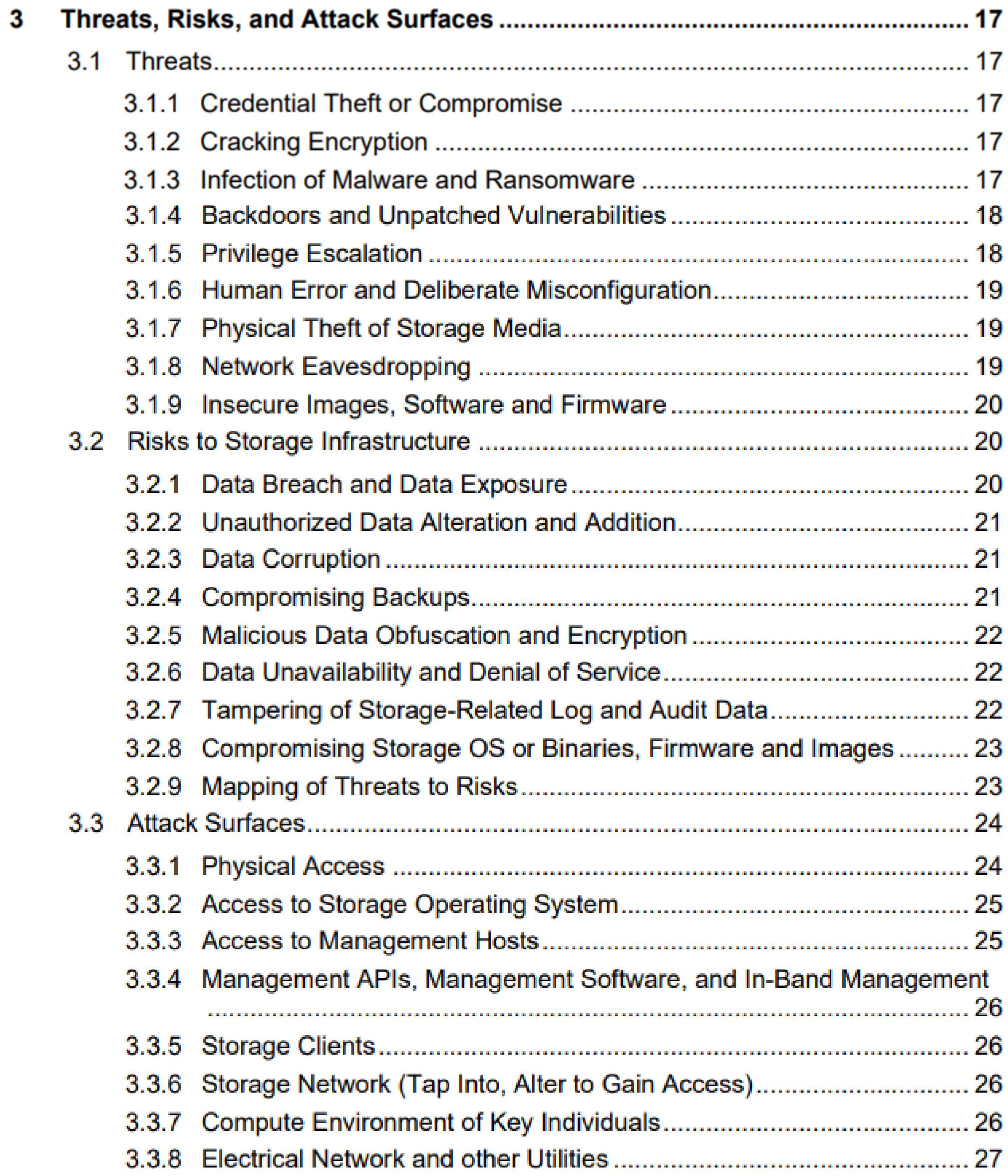
Example



NIST Special Publication 800-209

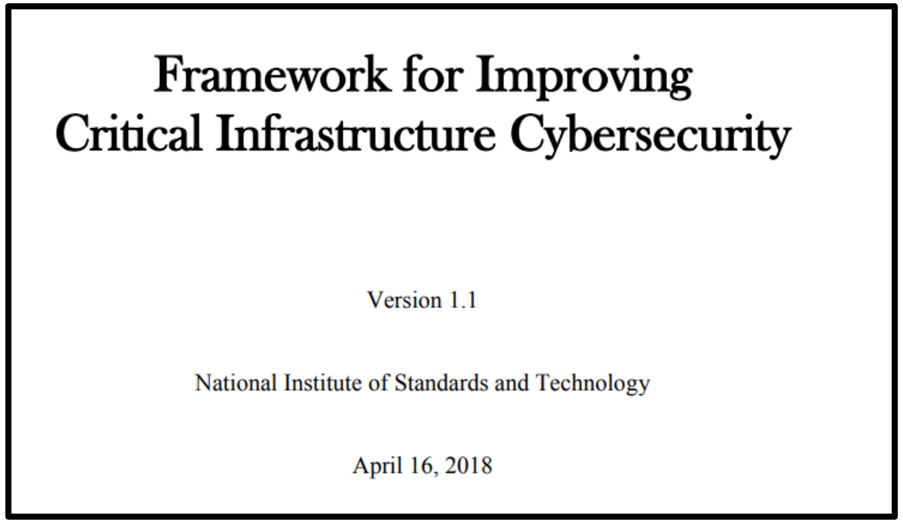
Security Guidelines for Storage Infrastructure

Ramaswamy Chandramouli
Doron Pinhas



Legal Exposures - *Frameworks*

Example



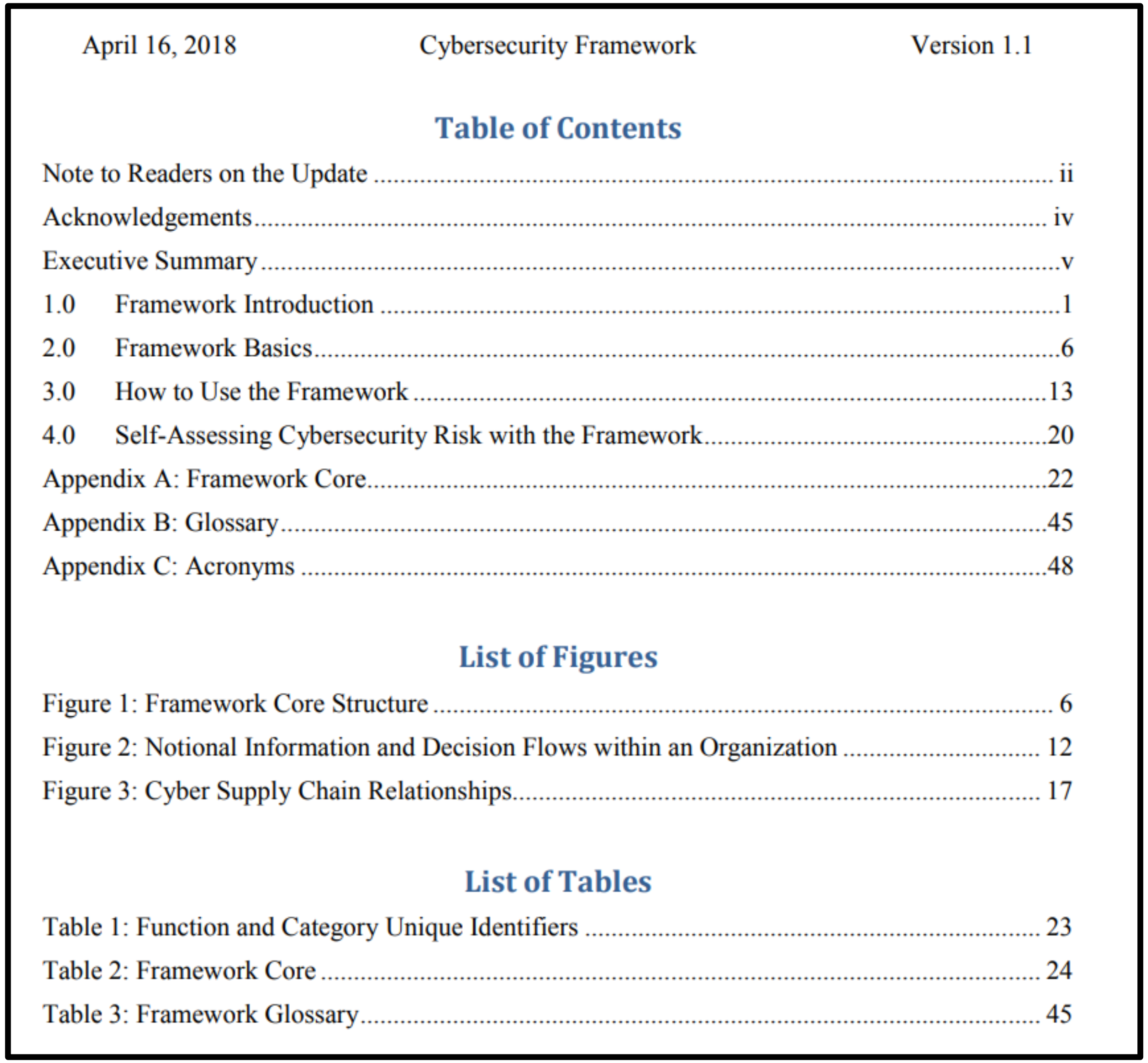
Framework for Improving Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018

https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf



April 16, 2018 Cybersecurity Framework Version 1.1

Table of Contents

List of Figures

List of Tables

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Legal Exposures – *Federal Agencies*

FTC Safeguards Rule – May 2022

- Requires covered financial institutions to develop, implement, and maintain an information security program with administrative, technical, and physical safeguards designed to protect customer information.
- Defines customer information to mean "any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates."
- Covers information about your own customers and information about customers of other financial institutions that have provided that data to you.

Must be written and it must be appropriate to the size and complexity of your business, the nature and scope of your activities, and the sensitivity of the information at issue. The objectives of your company's program are:

- to ensure the security and confidentiality of customer information;
- to protect against anticipated threats or hazards to the security or integrity of that information; and
- to protect against unauthorized access to that information that could result in substantial harm or inconvenience to any customer.

https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Legal Exposures – *Federal Agencies*

FTC Safeguards Rule – May 2022

- The Safeguards Rule applies to financial institutions subject to the FTC's jurisdiction and that aren't subject to the enforcement authority of another regulator under section 505 of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6805.
- According to Section 314.1(b), an entity is a "financial institution" if it's engaged in an activity that is "financial in nature" or is "incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C § 1843(k)."
- The Rule defines "financial institution" in a way that's broader than how people may use that phrase in conversation. Furthermore, what matters are the types of activities your business undertakes, not how you or others categorize your company.
- Examples of the kinds of entities that *are* financial institutions under the Rule, including mortgage lenders, payday lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, and investment advisors and finders that aren't required to register with the SEC.

https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Legal Exposures – ***Federal Agencies***

FTC Safeguards Rule – May 2022

What does a reasonable information security program look like?

1. *Designate a Qualified Individual to implement and supervise your company's information security program*
2. *Conduct a risk assessment*
3. *Design and implement safeguards to control the risks identified through your risk assessment*
4. *Regularly monitor and test the effectiveness of your safeguards*
5. *Train your staff*
6. *Monitor your service providers*
7. *Keep your information security program current*
8. *Create a written incident response plan*
9. *Require your Qualified Individual to report to your Board of Directors*

https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Legal Exposures – *Federal Agencies*

FTC Safeguards Rule – May 2022

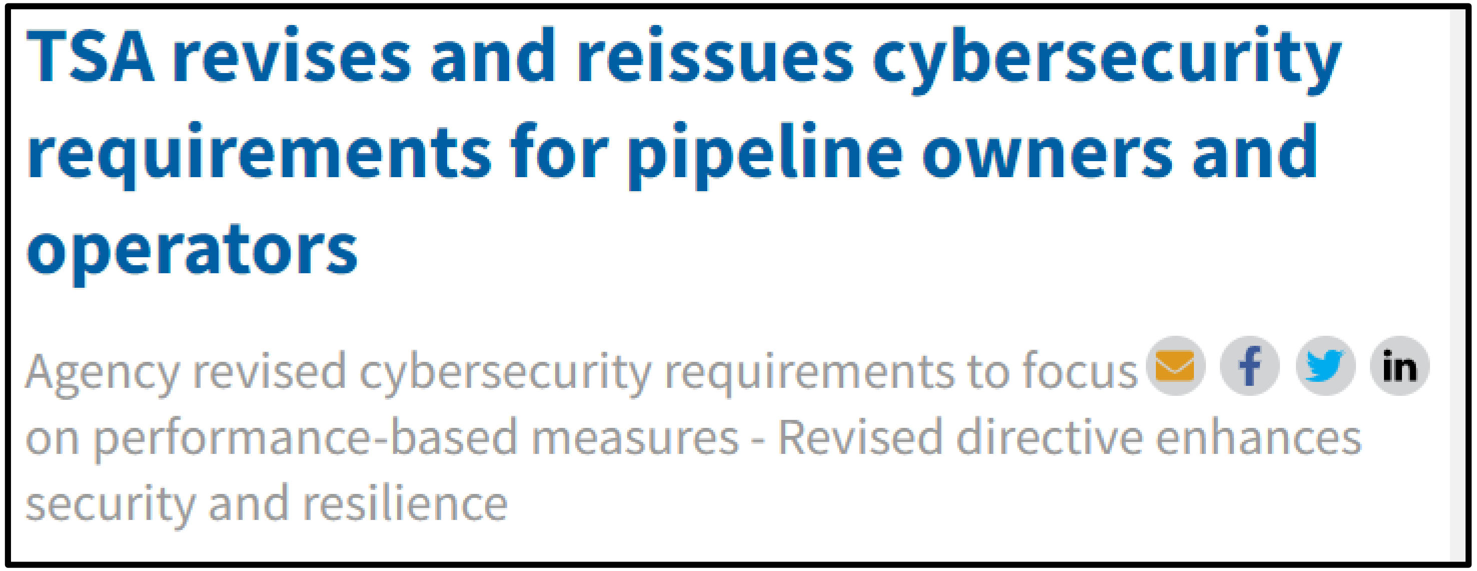
3. Design and implement safeguards to control the risks identified through your risk assessment

- Implement and periodically review access controls
- Know what you have and where you have it
- Encrypt customer information on your system and when it's in transit
- Assess your apps
- Implement multi-factor authentication for anyone accessing customer information on your system
- Dispose of customer information securely
- Anticipate and evaluate changes to your information system or network
- Maintain a log of authorized users' activity and keep an eye out for unauthorized access

https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know

Legal Exposures – *Federal Agencies*

7/21/2022



TSA revises and reissues cybersecurity requirements for pipeline owners and operators

Agency revised cybersecurity requirements to focus on performance-based measures - Revised directive enhances security and resilience

https://www.tsa.gov/news/press/releases/2022/07/21/tsa-revises-and-reissues-cybersecurity-requirements-pipeline-owners

Legal Exposures – ***Federal Agencies***

… Owner/Operators must do the following:

1. Establish and implement a TSA-approved Cybersecurity Implementation Plan that describes the specific cybersecurity measures employed and the schedule for achieving the outcomes described in Section III.A. through III.E.

2. Develop and maintain an up-to-date Cybersecurity Incident Response Plan to reduce the risk of operational disruption, or the risk of other significant impacts on necessary capacity, as defined in this Security Directive, should the Information and/or Operational Technology systems of a gas or liquid pipeline be affected by a cybersecurity incident. See Section III.F.

3. Establish a Cybersecurity Assessment Program and submit an annual plan that describes how the Owner/Operator will proactively and regularly assess the effectiveness of cybersecurity measures and identify and resolve device, network, and/or system vulnerabilities. See Section III.G

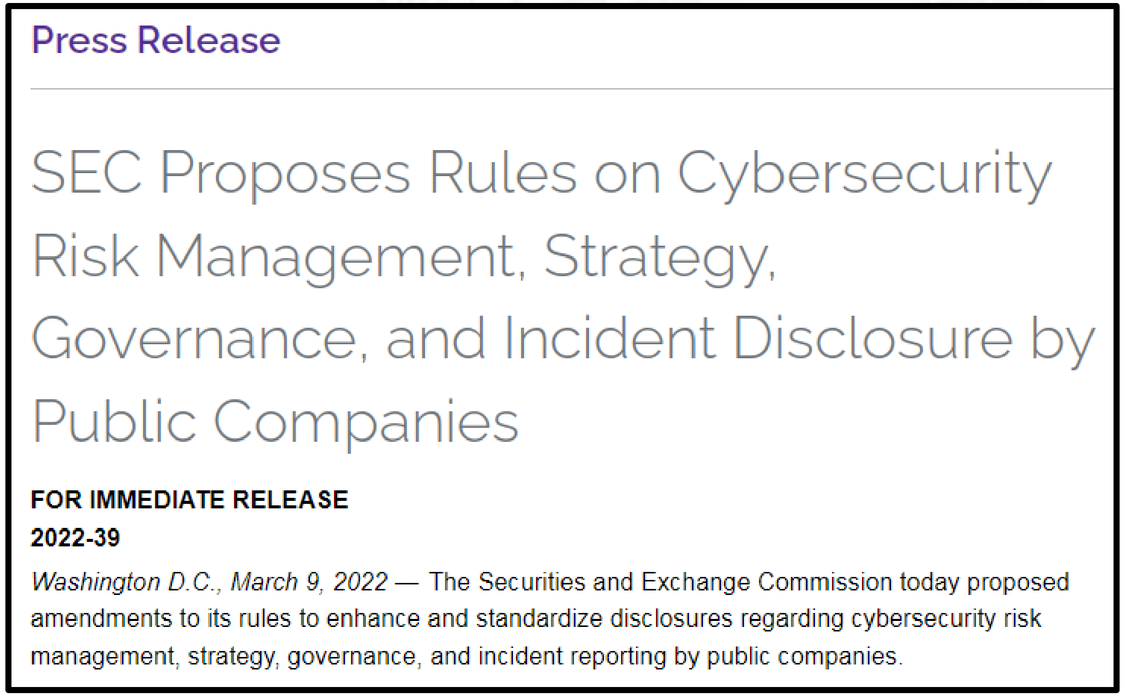
https://www.tsa.gov/sites/default/files/tsa_sd_pipeline-2021-02-july-21_2022.pdf

22 Pages

Legal Exposures – *Federal Agencies*

U.S. SECURITIES AND
EXCHANGE COMMISSION

3/9/2022



Press Release

SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies

FOR IMMEDIATE RELEASE

2022-39

Washington D.C., March 9, 2022 — The Securities and Exchange Commission today proposed amendments to its rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies.

https://www.sec.gov/news/press-release/2022-39

SEC Chair Gary Gensler Statement

U.S. SECURITIES AND
EXCHANGE COMMISSION

Today, cybersecurity is an emerging risk with which public issuers increasingly must contend. Investors want to know more about how issuers are managing those growing risks. …

- SEC Chair Gary Gensler

https://www.sec.gov/news/press-release/2022-39

SEC Vision, Mission, Values and Goals

U.S. SECURITIES AND
EXCHANGE COMMISSION

Vision The SEC strives to promote a market environment that is worthy of the public’s trust and characterized by transparency and integrity.

Mission The mission of the SEC is to protect investors; maintain fair, orderly, and efficient markets; and facilitate capital formation.

Values Integrity, Teamwork, Accountability, Fairness, Effectiveness, Commitment to Excellence

https://www.sec.gov/about/reports/sec-fy2014-agency-mission-information.pdf, Pg. 9

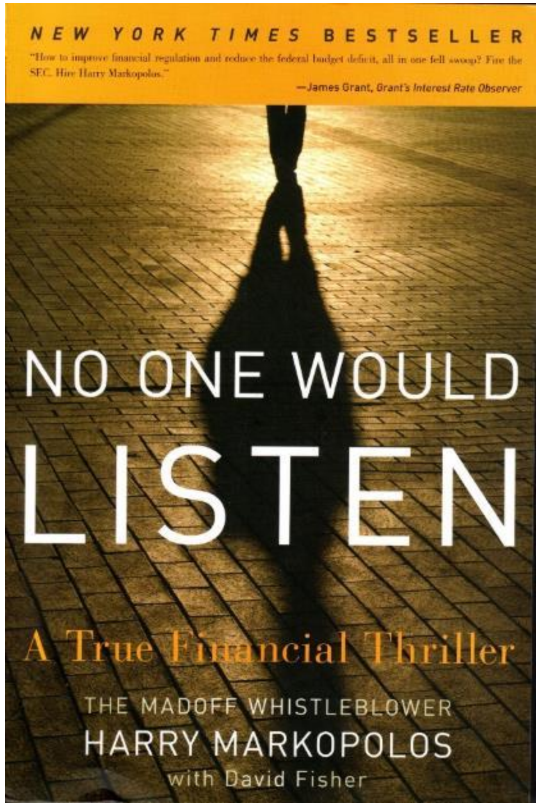
What Could Possibly Go Wrong?

Bernard Lawrence Madoff

https://www.npr.org/2021/04/14/987162416/bernie-madoff-financier-behind-notorious-ponzi-scheme-dies-at-age-82

Harry Markopolos

https://en.wikipedia.org/wiki/Harry_Markopolos#/media/File:Harry_Markopolos_on_C-SPAN.jpg


NEW YORK TIMES BESTSELLER
"How to improve financial regulation and reduce the federal budget deficit, all in one fell swoop? Fire the SEC. Hire Harry Markopolos."
—James Grant, Grant's Interest Rate Observer
NO ONE WOULD
LISTEN
A True Financial Thriller
THE MADOFF WHISTLEBLOWER
HARRY MARKOPOLOS
with David Fisher

Definition of a Mathematician

Someone who:

- Says *A*
- Means *B*
- Writes *C*

When the answer is *D*.

Prime Numbers

5 $\boxed{5 = 1 \times 5}$ $\boxed{\textit{Factors}: 1, 5}$

$\boxed{\text{5 is a } \textit{Prime Number}}$

---

6 $\boxed{6 = 1 \times 6 = 1 \times 2 \times 3}$ $\boxed{\textit{Factors}: 1, 2, 3, 6}$

$\boxed{\text{6 is } \textbf{not} \text{ a } \textit{Prime Number}}$

Fundamental Theorem of Arithmetic (a.k.a. Unique Factorization Theorem)

Every integer greater than 1 can be represented uniquely as a product of prime numbers.

Relatively Prime Numbers

15 = 1 x 3 x 5

Factors: 1, 3, 5

14 = 1 x 2 x 7

Factors: 1, 2, 7

14 and 15 are **not** Prime Numbers

14 and 15 only share *1* as a factor.

∴14 and 15 are *relatively* Prime Numbers

Modulo Mathematics Review

Modulo Examples

$$23 == 1(14) + \underline{9}$$

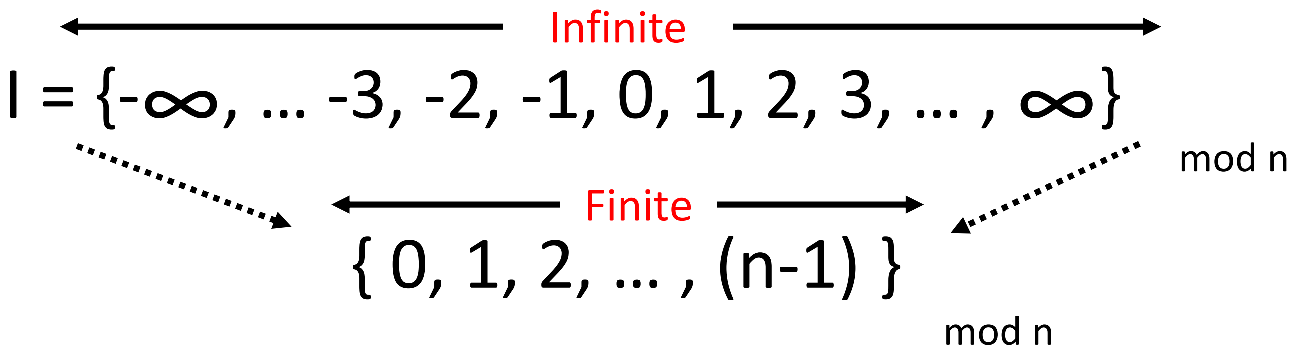
$$23_{\text{mod } 14} \equiv \underline{9}_{\text{mod } 14}$$

$$39 == 2(17) + \underline{5}$$

$$39_{(\text{mod } 17)} \equiv \underline{5}_{\text{mod } 17}$$

Modulo Mathematics Review (cont.)

So



Infinite

I = {-∞, … -3, -2, -1, 0, 1, 2, 3, … , ∞}

mod n

Finite

{ 0, 1, 2, … , (n-1) }

mod n

Modulo Mathematics Review (cont.)

Mod 7 Tables

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

N * 0 = 0

*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

All Non-zero Elements

- Because 7 is a prime number, 1 – 6 are *relatively* prime to 7
- ∴ Have a unique multiplicative inverse

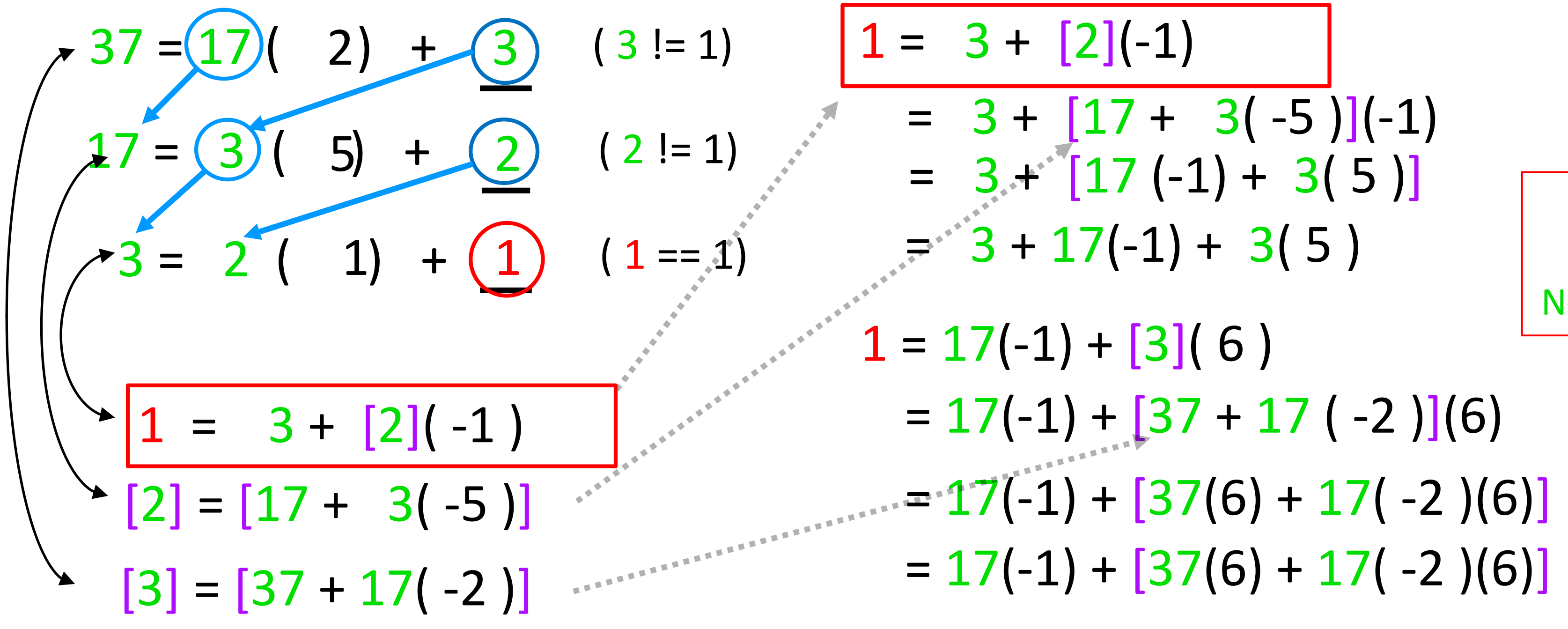
Prime numbers and multiplicative inverses are *very* important in cryptography

Modulo Mathematics Review (cont.)

The *Extended Euclidian Algorithm* Dynamically Calculates *Modulo N Multiplicative Inverses*

Example: $17_{\text{mod } 37}$, $(17_{\text{mod } 37})^{-1} == ?$

[If $(N*17)_{\text{mod } 37} == 1$, N == ?]



$37 = 17(\ 2) + \underline{3}$ (3 != 1)

$17 = 3(\ 5) + \underline{2}$ (2 != 1)

$3 = 2(\ 1) + \underline{1}$ (1 == 1)

$$\boxed{1 = 3 + [2](-1)}$$

$[2] = [17 + 3(-5)]$

$[3] = [37 + 17(-2)]$

$$\boxed{1 = 3 + [2](-1)}$$

$= 3 + [17 + 3(-5)](-1)$

$= 3 + [17(-1) + 3(5)]$

$= 3 + 17(-1) + 3(5)$

Do NOT Evaluate N*M Products

$1 = 17(-1) + [3](6)$

$= 17(-1) + [37 + 17(-2)](6)$

$= 17(-1) + [37(6) + 17(-2)(6)]$

$= 17(-1) + [37(6) + 17(-2)(6)]$

$1 = 37(6) + 17(-13)$?????

$1 = (222) - (221)$?????

Modulo Mathematics Review (cont.)

The *Extended Euclidian Algorithm* Dynamically Calculates *Modulo N Multiplicative Inverses*

Example: $17_{\text{mod } 37}$, $(17_{\text{mod } 37})^{-1}$ == ?

[If $(N*17)_{\text{mod } 37}$ == 1, N == ?]

$$1 = 37(6) + 17(-13)$$

$$1_{\text{mod } 37} = 0 + [\ 17(-13)\ ]_{\text{mod } 37} = [\ 17(24)\ ]_{\text{mod } 37}$$

$$1 = [\ 17(24)\ ]_{\text{mod } 37}$$

$$(17_{\text{mod } 37})^{-1} == 24$$

Check:

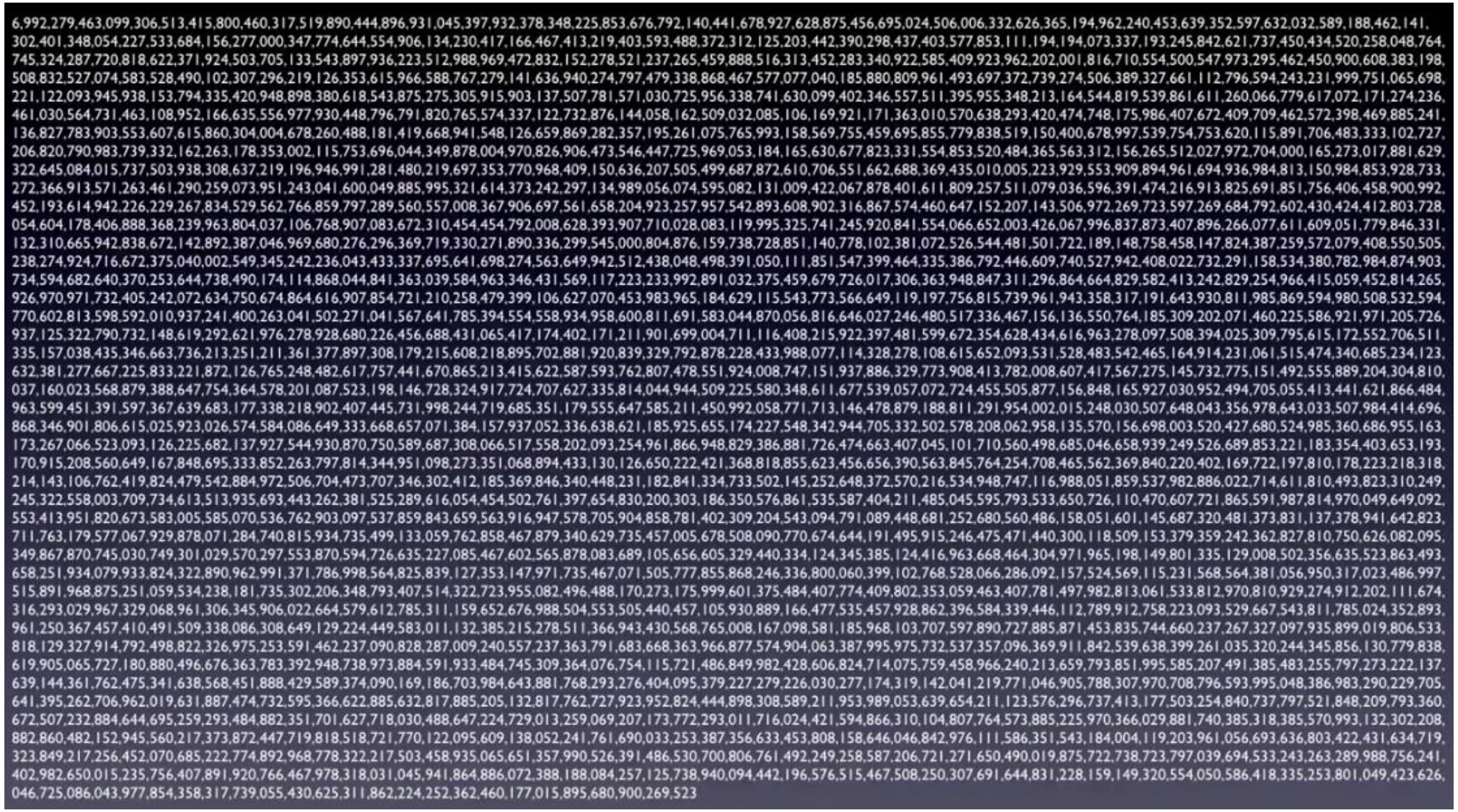
$$\frac{(17)(24)}{37} = 11 + (\text{Remainder} == 1)$$

RSA Encryption Introduction

Message to encrypt *m* is a *NUMBER*.

Let *e* and *N* be numbers the decrypter provides

N is very large



```
6,992,279,463,099,306,513,415,800,460,317,519,890,444,896,931,045,397,932,378,348,225,853,676,792,140,441,678,927,628,875,456,695,024,506,006,332,626,365,194,962,240,453,639,352,597,632,032,589,188,462,141,
302,401,348,054,227,533,684,156,277,000,347,774,644,554,906,134,230,417,166,467,413,219,403,593,488,372,312,125,203,442,390,298,437,403,577,853,111,194,194,073,337,193,245,842,621,737,450,434,520,258,048,764,
745,324,287,720,818,622,371,924,503,705,133,543,897,936,223,512,988,969,472,832,152,278,521,237,265,459,888,516,313,452,283,340,922,585,409,923,962,202,001,816,710,554,500,547,973,295,462,450,900,608,383,198,
508,832,527,074,583,528,490,102,307,296,219,126,353,615,966,588,767,279,141,636,940,274,797,479,338,868,467,577,077,040,185,880,809,961,493,697,372,739,274,506,389,327,661,112,796,594,243,231,999,751,065,698,
221,122,093,945,938,153,794,335,420,948,898,380,618,543,875,275,305,915,903,137,507,781,571,030,725,956,338,741,630,099,402,346,557,511,395,955,348,213,164,544,819,539,861,611,260,066,779,617,072,171,274,236,
461,030,564,731,463,108,952,166,635,556,977,930,448,796,791,820,765,574,337,122,732,876,144,058,162,509,032,085,106,169,921,171,363,010,570,638,293,420,474,748,175,986,407,672,409,709,462,572,398,469,885,241,
136,827,783,903,553,607,615,860,304,004,678,260,488,181,419,668,941,548,126,659,869,282,357,195,261,075,765,993,158,569,755,459,695,855,779,838,519,150,400,678,997,539,754,753,620,115,891,706,483,333,102,727,
206,820,790,983,739,332,162,263,178,353,002,115,753,696,044,349,878,004,970,826,906,473,546,447,725,969,053,184,165,630,677,823,331,554,853,520,484,365,563,312,156,265,512,027,972,704,000,165,273,017,881,629,
322,645,084,015,737,503,938,308,637,219,196,946,991,281,480,219,697,353,770,968,409,150,636,207,505,499,687,872,610,706,551,662,688,369,435,010,005,223,929,553,909,894,961,694,936,984,813,150,984,853,928,733,
272,366,913,571,263,461,290,259,073,951,243,041,600,049,885,995,321,614,373,242,297,134,989,056,074,595,082,131,009,422,067,878,401,611,809,257,511,079,036,596,391,474,216,913,825,691,851,756,406,458,900,992,
452,193,614,942,226,229,267,834,529,562,766,859,797,289,560,557,008,367,906,697,561,658,204,923,257,957,542,893,608,902,316,867,574,460,647,152,207,143,506,972,269,723,597,269,684,792,602,430,424,412,803,728,
054,604,178,406,888,368,239,963,804,037,106,768,907,083,672,310,454,454,792,008,628,393,907,710,028,083,119,995,325,741,245,920,841,554,066,652,003,426,067,996,837,873,407,896,266,077,611,609,051,779,846,331,
132,310,665,942,838,672,142,892,387,046,969,680,276,296,369,719,330,271,890,336,299,545,000,804,876,159,738,728,851,140,778,102,381,072,526,544,481,501,722,189,148,758,458,147,824,387,259,572,079,408,550,505,
238,274,924,716,672,375,040,002,549,345,242,236,043,433,337,695,641,698,274,563,649,942,512,438,048,498,391,050,111,851,547,399,464,335,386,792,446,609,740,527,942,408,022,732,291,158,534,380,782,984,874,903,
734,594,682,640,370,253,644,738,490,174,114,868,044,841,363,039,584,963,346,431,569,117,223,233,992,891,032,375,459,679,726,017,306,363,948,847,311,296,864,664,829,582,413,242,829,254,966,415,059,452,814,265,
926,970,971,732,405,242,072,634,750,674,864,616,907,854,721,210,258,479,399,106,627,070,453,983,965,184,629,115,543,773,566,649,119,197,756,815,739,961,943,358,317,191,643,930,811,985,869,594,980,508,532,594,
770,602,813,598,592,010,937,241,400,263,041,502,271,041,567,641,785,394,554,558,934,958,600,811,691,583,044,870,056,816,646,027,246,480,517,336,467,156,136,550,764,185,309,202,071,460,225,586,921,971,205,726,
937,125,322,790,732,148,619,292,621,976,278,928,680,226,456,688,431,065,417,174,402,171,211,901,699,004,711,116,408,215,922,397,481,599,672,354,628,434,616,963,278,097,508,394,025,309,795,615,172,552,706,511,
335,157,038,435,346,663,736,213,251,211,361,377,897,308,179,215,608,218,895,702,881,920,839,329,792,878,228,433,988,077,114,328,278,108,615,652,093,531,528,483,542,465,164,914,231,061,515,474,340,685,234,123,
632,381,277,667,225,833,221,872,126,765,248,482,617,757,441,670,865,213,415,622,587,593,762,807,478,551,924,008,747,151,937,886,329,773,908,413,782,008,607,417,567,275,145,732,775,151,492,555,889,204,304,810,
037,160,023,568,879,388,647,754,364,578,201,087,523,198,146,728,324,917,724,707,627,335,814,044,944,509,225,580,348,611,677,539,057,072,724,455,505,877,156,848,165,927,030,952,494,705,055,413,441,621,866,484,
963,599,451,391,597,367,639,683,177,338,218,902,407,445,731,998,244,719,685,351,179,555,647,585,211,450,992,058,771,713,146,478,879,188,811,291,954,002,015,248,030,507,648,043,356,978,643,033,507,984,414,696,
868,346,901,806,615,025,923,026,574,584,086,649,333,668,657,071,384,157,937,052,336,638,621,185,925,655,174,227,548,342,944,705,332,502,578,208,062,958,135,570,156,698,003,520,427,680,524,985,360,686,955,163,
173,267,066,523,093,126,225,682,137,927,544,930,870,750,589,687,308,066,517,558,202,093,254,961,866,948,829,386,881,726,474,663,407,045,101,710,560,498,685,046,658,939,249,526,689,853,221,183,354,403,653,193,
170,915,208,560,649,167,848,695,333,852,263,797,814,344,951,098,273,351,068,894,433,130,126,650,222,421,368,818,855,623,456,656,390,563,845,764,254,708,465,562,369,840,220,402,169,722,197,810,178,223,218,318,
214,143,106,762,419,824,479,542,884,972,506,704,473,707,346,302,412,185,369,846,340,448,231,182,841,334,733,502,145,252,648,372,570,216,534,948,747,116,988,051,859,537,982,886,022,714,611,810,493,823,310,249,
245,322,558,003,709,734,613,513,935,693,443,262,381,525,289,616,054,454,502,761,397,654,830,200,303,186,350,576,861,535,587,404,211,485,045,595,793,533,650,726,110,470,607,721,865,591,987,814,970,049,649,092,
553,413,951,820,673,583,005,585,070,536,762,903,097,537,859,843,659,563,916,947,578,705,904,858,781,402,309,204,543,094,791,089,448,681,252,680,560,486,158,051,601,145,687,320,481,373,831,137,378,941,642,823,
711,763,179,577,067,929,878,071,284,740,815,934,735,499,133,059,762,858,467,879,340,629,735,457,005,678,508,090,770,674,644,191,495,915,246,475,471,440,300,118,509,153,379,359,242,362,827,810,750,626,082,095,
349,867,870,745,030,749,301,029,570,297,553,870,594,726,635,227,085,467,602,565,878,083,689,105,656,605,329,440,334,124,345,385,124,416,963,668,464,304,971,965,198,149,801,335,129,008,502,356,635,523,863,493,
658,251,934,079,933,824,322,890,962,991,371,786,998,564,825,839,127,353,147,971,735,467,071,505,777,855,868,246,336,800,060,399,102,768,528,066,286,092,157,524,569,115,231,568,564,381,056,950,317,023,486,997,
515,891,968,875,251,059,534,238,181,735,302,206,348,793,407,514,322,723,955,082,496,488,170,273,175,999,601,375,484,407,774,409,802,353,059,463,407,781,497,982,813,061,533,812,970,810,929,274,912,202,111,674,
316,293,029,967,329,068,961,306,345,906,022,664,579,612,785,311,159,652,676,988,504,553,505,440,457,105,930,889,166,477,535,457,928,862,396,584,339,446,112,789,912,758,223,093,529,667,543,811,785,024,352,893,
961,250,367,457,410,491,509,338,086,308,649,129,224,449,583,011,132,385,215,278,511,366,943,430,568,765,008,167,098,581,185,968,103,707,597,890,727,885,871,453,835,744,660,237,267,327,097,935,899,019,806,533,
818,129,327,914,792,498,822,326,975,253,591,462,237,090,828,287,009,240,557,237,363,791,683,668,363,966,877,574,904,063,387,995,975,732,537,357,096,369,911,842,539,638,399,261,035,320,244,345,856,130,779,838,
619,905,065,727,180,880,496,676,363,783,392,948,738,973,884,591,933,484,745,309,364,076,754,115,721,486,849,982,428,606,824,714,075,759,458,966,240,213,659,793,851,995,585,207,491,385,483,255,797,273,222,137,
639,144,361,762,475,341,638,568,451,888,429,589,374,090,169,186,703,984,643,881,768,293,276,404,095,379,227,279,226,030,277,174,319,142,041,219,771,046,905,788,307,970,708,796,593,995,048,386,983,290,229,705,
641,395,262,706,962,019,631,887,474,732,595,366,622,885,632,817,885,205,132,817,762,727,923,952,824,444,898,308,589,211,953,989,053,639,654,211,123,576,296,737,413,177,503,254,840,737,797,521,848,209,793,360,
672,507,232,884,644,695,259,293,484,882,351,701,627,718,030,488,647,224,729,013,259,069,207,173,772,293,011,716,024,421,594,866,310,104,807,764,573,885,225,970,366,029,881,740,385,318,385,570,993,132,302,208,
882,860,482,152,945,560,217,373,872,447,719,818,518,721,770,122,095,609,138,052,241,761,690,033,253,387,356,633,453,808,158,646,046,842,976,111,586,351,543,184,004,119,203,961,056,693,636,803,422,431,634,719,
323,849,217,256,452,070,685,222,774,892,968,778,322,217,503,458,935,065,651,357,990,526,391,486,530,700,806,761,492,249,258,587,206,721,271,650,490,019,875,722,738,723,797,039,694,533,243,263,289,988,756,241,
402,982,650,015,235,756,407,891,920,766,467,978,318,031,045,941,864,886,072,388,188,084,257,125,738,940,094,442,196,576,515,467,508,250,307,691,644,831,228,159,149,320,554,050,586,418,335,253,801,049,423,626,
046,725,086,043,977,854,358,317,739,055,430,625,311,862,224,252,362,460,177,015,895,680,900,269,523
```

https://www.youtube.com/watch?v=Z8M2BTscoD4&t=10s

RSA Encryption Introduction

Decrypter provides

- *e* (large and carefully selected)
- *n* (*very* large, ~ 4,000 bits)

Message to encrypt *m* is a *NUMBER* < *n*

Encryption: $m' = m^{e}{}_{\text{mod } n}$

Let *d* (computed & secret) = $e^{-1}{}_{\text{mod } n}$

Decryption: $(m')^{d}{}_{\text{mod } n} = m^{e * d} = m^{e * e^{-1}} = m^{e^{0}} = m^{1} = m$

e and *d* are different values ⇒ *Asymmetric Encryption*

RSA Encryption Toy Example

p = 5 (large prime, secret)
q = 11 (large prime , secret)
n = p*q = 5 * 11 = 55

$$\begin{aligned}\Phi(55) &= \Phi(5) * \Phi(11)\\ &= 4 * 10\\ &= 40 \quad \text{(secret)}\end{aligned}$$

$V_0 = 40,\ V_1 = 7$

Pick *e* so that gcd(*e*, 40) = 1

$40 = 2^3 * 5$

$e = 7 \qquad \gcd(7, 40) = 1$

$\therefore\ e^{-1} \bmod 40$ exists

$d = e^{-1} \Rightarrow e * d = e * e^{-1} = 1$

Least Residue System Modulo 40

~~0~~	~~10~~	~~20~~	~~30~~
1	11	21	31
~~2~~	~~12~~	~~22~~	~~32~~
3	13	23	33
~~4~~	~~14~~	~~24~~	~~34~~
~~5~~	~~15~~	~~25~~	~~35~~
~~6~~	~~16~~	~~26~~	~~36~~
$\boxed{7}$	17	27	37
~~8~~	~~18~~	~~28~~	~~38~~
9	19	29	39

40 – 24 = 16 Relatively Prime Numbers

$$\left.\begin{aligned}\overset{V_0}{40} &= 5 * \overset{V_1}{7} + \overset{V_2}{5}\\ \overset{V_1}{7} &= 1 * \overset{V_2}{5} + \overset{V_3}{2}\\ \overset{V_2}{5} &= 2 * \overset{V_3}{2} + \boxed{1}\end{aligned}\right\} \quad \left.\begin{aligned}V_0 &= 5 * V_1 + V_2\\ V_1 &= 1 * V_2 + V_3\\ V_2 &= 2 * V_3 + \boxed{1}\end{aligned}\right\} \quad \left.\begin{aligned}V_0 - 5 * V_1 &= V_2\\ V_1 - 1 * V_2 &= V_3\\ V_2 - 2 * V_3 &= \boxed{1}\end{aligned}\right\}$$

RSA Encryption Toy Example

$p = 5$ (large prime, secret)
$q = 11$ (large prime , secret)
$n = p*q = 5 * 11 = 55$

$$\begin{aligned}\Phi(55) &= \Phi(5) * \Phi(11)\\ &= 4 * 10\\ &= 40 \quad \text{(secret)}\end{aligned}$$

$V_0 = 40,\ V_1 = 7$

Pick e so that $\gcd(e, 40) = 1$

$40 = 2^3 * 5$

$e = 7 \qquad \gcd(7, 40) = 1$

$\therefore\ e^{-1} \bmod 40$ exists

$d = e^{-1} \Rightarrow e * d = e * e^{-1} = 1$

Least Residue System Modulo 40

~~0~~	~~10~~	~~20~~	~~30~~
1	11	21	31
~~2~~	~~12~~	~~22~~	~~32~~
3	13	23	33
~~4~~	~~14~~	~~24~~	~~34~~
~~5~~	~~15~~	~~25~~	~~35~~
~~6~~	~~16~~	~~26~~	~~36~~
[✓ 7]	17	27	37
~~8~~	~~18~~	~~28~~	~~38~~
9	19	29	39

40 – 24 = 16 Relatively Prime Numbers

$$\left.\begin{aligned} V_0 - 5 * V_1 &= V_2\\ V_1 - 1 * V_2 &= V_3\\ V_2 - 2 * V_3 &= \boxed{1}\end{aligned}\right\} \quad \left.\begin{aligned} V_2 &= V_0 - 5 * V_1\\ V_3 &= V_1 - 1 * V_2\\ \boxed{1} &= V_2 - 2 * V_3\end{aligned}\right\} \quad \left.\begin{aligned} \boxed{1} &= V_2 - 2 * V_3\\ V_3 &= V_1 - 1 * V_2\\ V_2 &= V_0 - 5 * V_1\end{aligned}\right\}$$

RSA Encryption Toy Example

$p = 5$ (large prime, secret)
$q = 11$ (large prime , secret)
$n = p*q = 5 * 11 = 55$

$$\begin{aligned}\Phi(55) &= \Phi(5) * \Phi(11)\\ &= 4 * 10\\ &= 40 \quad \text{(secret)}\end{aligned}$$

Pick *e* so that gcd(*e*, 40) = 1

$40 = 2^3 * 5$

$e = 7 \qquad \gcd(7, 40) = 1$

$\therefore\ e^{-1} \bmod 40$ exists

$d = e^{-1} \Rightarrow e * d = e * e^{-1} = 1$

Least Residue System Modulo 40

~~0~~	~~10~~	~~20~~	~~30~~
1	11	21	31
~~2~~	~~12~~	~~22~~	~~32~~
3	13	23	33
~~4~~	~~14~~	~~24~~	~~34~~
~~5~~	~~15~~	~~25~~	~~35~~
~~6~~	~~16~~	~~26~~	~~36~~
[✓ 7]	17	27	37
~~8~~	~~18~~	~~28~~	~~38~~
9	19	29	39

40 – 24 = 16 Relatively Prime Numbers

$V_0 = 40,\ V_1 = 7$

$1 = V_2 - 2 * V_3$

$V_3 = V_1 - 1 * V_2$

$V_2 = V_0 - 5 * V_1$

$$\begin{aligned}1 &= V_2 - 2 * [V_1 - V_2] = 3V_2 - 2V_1\\ &= 3[V_0 - 5V_1] - 2V_1\\ &= 3V_0 - 17V_1\\ &= 3(40) + (-17)(7)\end{aligned}$$

$\therefore\ 1 = (-17)e \bmod 40$

$\therefore\ d = (-17) \bmod 40$

$\therefore\ d = (23) \bmod 40$ (secret)

Check: $(23 * 7) \bmod 40 = 161 \bmod 40$
$= 1 \bmod 40$

RSA Encryption Toy Example

$p = 5$ (large prime, secret)
$q = 11$ (large prime , secret)
$n = p*q = 5 * 11 = 55$

$$\begin{aligned}\Phi(55) &= \Phi(5) * \Phi(11)\\ &= 4 * 10\\ &= 40 \quad \text{(secret)}\end{aligned}$$

$V_0 = 40, V_1 = 7$

Pick *e* so that gcd(*e*, 40) = 1

$40 = 2^3 * 5$

$e = 7 \qquad \gcd(7, 40) = 1$

$\therefore\ e^{-1} \bmod 40$ exists

$d = e^{-1} \Rightarrow e * d = e * e^{-1} = 1$

Least Residue System Modulo 40

~~0~~	~~10~~	~~20~~	~~30~~
1	11	21	31
~~2~~	~~12~~	~~22~~	~~32~~
3	13	23	33
~~4~~	~~14~~	~~24~~	~~34~~
~~5~~	~~15~~	~~25~~	~~35~~
~~6~~	~~16~~	~~26~~	~~36~~
7	17	27	37
~~8~~	~~18~~	~~28~~	~~38~~
9	19	29	39

40 – 24 = 16 Relatively Prime Numbers

Example: Encrypt/Decrypt $m = 28 < 55 = n$

Encrypt $m = 28 \Rightarrow m' = m^{e} \bmod n = 28^{7} \bmod 55 = 52 = m'$

Decrypt $m' = 52 \Rightarrow m = m'^{d} \bmod n = 52^{23} \bmod 55 = 28 = m$ ✓

What Does Quantum Computing Do?

Shor’s Algorithm Iteratively Factors Large Numbers

6,992,279,463,099,306,513,415,800,460,317,519,890,444,896,931,045,397,932,378,348,225,853,676,792,140,441,678,927,628,875,456,695,024,506,006,332,626,365,194,962,240,453,639,352,597,632,032,589,188,462,141,
302,401,348,054,227,533,684,156,277,000,347,774,644,554,906,134,230,417,166,467,413,219,403,593,488,372,312,125,203,442,390,298,437,403,577,853,111,194,194,073,337,193,245,842,621,737,450,434,520,258,048,764,
745,324,287,720,818,622,371,924,503,705,133,543,897,936,223,512,988,969,472,832,152,278,521,237,265,459,888,516,313,452,283,340,922,585,409,923,962,202,001,816,710,554,500,547,973,295,462,450,900,608,383,198,
508,832,527,074,583,528,490,102,307,296,219,126,353,615,966,588,767,279,141,636,940,274,797,479,338,868,467,577,077,040,185,880,809,961,493,697,372,739,274,506,389,327,661,112,796,594,243,231,999,751,065,698,
221,122,093,945,938,153,794,335,420,948,898,380,618,543,875,275,305,915,903,137,507,781,571,030,725,956,338,741,630,099,402,346,557,511,395,955,348,213,164,544,819,539,861,611,260,066,779,617,072,171,274,236,
461,030,564,731,463,108,952,166,635,556,977,930,448,796,791,820,765,574,337,122,732,876,144,058,162,509,032,085,106,169,921,171,363,010,570,638,293,420,474,748,175,986,407,672,409,709,462,572,398,469,885,241,
136,827,783,903,553,607,615,860,304,004,678,260,488,181,419,668,941,548,126,659,869,282,357,195,261,075,765,993,158,569,755,459,695,855,779,838,519,150,400,678,997,539,754,753,620,115,891,706,483,333,102,727,
206,820,790,983,739,332,162,263,178,353,002,115,753,696,044,349,878,004,970,826,906,473,546,447,725,969,053,184,165,630,677,823,331,554,853,520,484,365,563,312,156,265,512,027,972,704,000,165,273,017,881,629,
322,645,084,015,737,503,938,308,637,219,196,946,991,281,480,219,697,353,770,968,409,150,636,207,505,499,687,872,610,706,551,662,688,369,435,010,005,223,929,553,909,894,961,694,936,984,813,150,984,853,928,733,
272,366,913,571,263,461,290,259,073,951,243,041,600,049,885,995,321,614,373,242,297,134,989,056,074,595,082,131,009,422,067,878,401,611,809,257,511,079,036,596,391,474,216,913,825,691,851,756,406,458,900,992,
452,193,614,942,226,229,267,834,529,562,766,859,797,289,560,557,008,367,906,697,561,658,204,923,257,957,542,893,608,902,316,867,574,460,647,152,207,143,506,972,269,723,597,269,684,792,602,430,424,412,803,728,
054,604,178,406,888,368,239,963,804,037,106,768,907,083,672,310,454,454,792,008,628,393,907,710,028,083,119,995,325,741,245,920,841,554,066,652,003,426,067,996,837,873,407,896,266,077,611,609,051,779,846,331,
132,310,665,942,838,672,142,892,387,046,969,680,276,296,369,719,330,271,890,336,299,545,000,804,876,159,738,728,851,140,778,102,381,072,526,544,481,501,722,189,148,758,458,147,824,387,259,572,079,408,550,505,
238,274,924,716,672,375,040,002,549,345,242,236,043,433,337,695,641,698,274,563,649,942,512,438,048,498,391,050,111,851,547,399,464,335,386,792,446,609,740,527,942,408,022,732,291,158,534,380,782,984,874,903,
734,594,682,640,370,253,644,738,490,174,114,868,044,841,363,039,584,963,346,431,569,117,223,233,992,891,032,375,459,679,726,017,306,363,948,847,311,296,864,664,829,582,413,242,829,254,966,415,059,452,814,265,
926,970,971,732,405,242,072,634,750,674,864,616,907,854,721,210,258,479,399,106,627,070,453,983,965,184,629,115,543,773,566,649,119,197,756,815,739,961,943,358,317,191,643,930,811,985,869,594,980,508,532,594,
770,602,813,598,592,010,937,241,400,263,041,502,271,041,567,641,785,394,554,558,934,958,600,811,691,583,044,870,056,816,646,027,246,480,517,336,467,156,136,550,764,185,309,202,071,460,225,586,921,971,205,726,
937,125,322,790,732,148,619,292,621,976,278,928,680,226,456,688,431,065,417,174,402,171,211,901,699,004,711,116,408,215,922,397,481,599,672,354,628,434,616,963,278,097,508,394,025,309,795,615,172,552,706,511,
335,157,038,435,346,663,736,213,251,211,361,377,897,308,179,215,608,218,895,702,881,920,839,329,792,878,228,433,988,077,114,328,278,108,615,652,093,531,528,483,542,465,164,914,231,061,515,474,340,685,234,123,
632,381,277,667,225,833,221,872,126,765,248,482,617,757,441,670,865,213,415,622,587,593,762,807,478,551,924,008,747,151,937,886,329,773,908,413,782,008,607,417,567,275,145,732,775,151,492,555,889,204,304,810,
037,160,023,568,879,388,647,754,364,578,201,087,523,198,146,728,324,917,724,707,627,335,814,044,944,509,225,580,348,611,677,539,057,072,724,455,505,877,156,848,165,927,030,952,494,705,055,413,441,621,866,484,
963,599,451,391,597,367,639,683,177,338,218,902,407,445,731,998,244,719,685,351,179,555,647,585,211,450,992,058,771,713,146,478,879,188,811,291,954,002,015,248,030,507,648,043,356,978,643,033,507,984,414,696,
868,346,901,806,615,025,923,026,574,584,086,649,333,668,657,071,384,157,937,052,336,638,621,185,925,655,174,227,548,342,944,705,332,502,578,208,062,958,135,570,156,698,003,520,427,680,524,985,360,686,955,163,
173,267,066,523,093,126,225,682,137,927,544,930,870,750,589,687,308,066,517,558,202,093,254,961,866,948,829,386,881,726,474,663,407,045,101,710,560,498,685,046,658,939,249,526,689,853,221,183,354,403,653,193,
170,915,208,560,649,167,848,695,333,852,263,797,814,344,951,098,273,351,068,894,433,130,126,650,222,421,368,818,855,623,456,656,390,563,845,764,254,708,465,562,369,840,220,402,169,722,197,810,178,223,218,318,
214,143,106,762,419,824,479,542,884,972,506,704,473,707,346,302,412,185,369,846,340,448,231,182,841,334,733,502,145,252,648,372,570,216,534,948,747,116,988,051,859,537,982,886,022,714,611,810,493,823,310,249,
245,322,558,003,709,734,613,513,935,693,443,262,381,525,289,616,054,454,502,761,397,654,830,200,303,186,350,576,861,535,587,404,211,485,045,595,793,533,650,726,110,470,607,721,865,591,987,814,970,049,649,092,
553,413,951,820,673,583,005,585,070,536,762,903,097,537,859,843,659,563,916,947,578,705,904,858,781,402,309,204,543,094,791,089,448,681,252,680,560,486,158,051,601,145,687,320,481,373,831,137,378,941,642,823,
711,763,179,577,067,929,878,071,284,740,815,934,735,499,133,059,762,858,467,879,340,629,735,457,005,678,508,090,770,674,644,191,495,915,246,475,471,440,300,118,509,153,379,359,242,362,827,810,750,626,082,095,
349,867,870,745,030,749,301,029,570,297,553,870,594,726,635,227,085,467,602,565,878,083,689,105,656,605,329,440,334,124,345,385,124,416,963,668,464,304,971,965,198,149,801,335,129,008,502,356,635,523,863,493,
658,251,934,079,933,824,322,890,962,991,371,786,998,564,825,839,127,353,147,971,735,467,071,505,777,855,868,246,336,800,060,399,102,768,528,066,286,092,157,524,569,115,231,568,564,381,056,950,317,023,486,997,
515,891,968,875,251,059,534,238,181,735,302,206,348,793,407,514,322,723,955,082,496,488,170,273,175,999,601,375,484,407,774,409,802,353,059,463,407,781,497,982,813,061,533,812,970,810,929,274,912,202,111,674,
316,293,029,967,329,068,961,306,345,906,022,664,579,612,785,311,159,652,676,988,504,553,505,440,457,105,930,889,166,477,535,457,928,862,396,584,339,446,112,789,912,758,223,093,529,667,543,811,785,024,352,893,
961,250,367,457,410,491,509,338,086,308,649,129,224,449,583,011,132,385,215,278,511,366,943,430,568,765,008,167,098,581,185,968,103,707,597,890,727,885,871,453,835,744,660,237,267,327,097,935,899,019,806,533,
818,129,327,914,792,498,822,326,975,253,591,462,237,090,828,287,009,240,557,237,363,791,683,668,363,966,877,574,904,063,387,995,975,732,537,357,096,369,911,842,539,638,399,261,035,320,244,345,856,130,779,838,
619,905,065,727,180,880,496,676,363,783,392,948,738,973,884,591,933,484,745,309,364,076,754,115,721,486,849,982,428,606,824,714,075,759,458,966,240,213,659,793,851,995,585,207,491,385,483,255,797,273,222,137,
639,144,361,762,475,341,638,568,451,888,429,589,374,090,169,186,703,984,643,881,768,293,276,404,095,379,227,279,226,030,277,174,319,142,041,219,771,046,905,788,307,970,708,796,593,995,048,386,983,290,229,705,
641,395,262,706,962,019,631,887,474,732,595,366,622,885,632,817,885,205,132,817,762,727,923,952,824,444,898,308,589,211,953,989,053,639,654,211,123,576,296,737,413,177,503,254,840,737,797,521,848,209,793,360,
672,507,232,884,644,695,259,293,484,882,351,701,627,718,030,488,647,224,729,013,259,069,207,173,772,293,011,716,024,421,594,866,310,104,807,764,573,885,225,970,366,029,881,740,385,318,385,570,993,132,302,208,
882,860,482,152,945,560,217,373,872,447,719,818,518,721,770,122,095,609,138,052,241,761,690,033,253,387,356,633,453,808,158,646,046,842,976,111,586,351,543,184,004,119,203,961,056,693,636,803,422,431,634,719,
323,849,217,256,452,070,685,222,774,892,968,778,322,217,503,458,935,065,651,357,990,526,391,486,530,700,806,761,492,249,258,587,206,721,271,650,490,019,875,722,738,723,797,039,694,533,243,263,289,988,756,241,
402,982,650,015,235,756,407,891,920,766,467,978,318,031,045,941,864,886,072,388,188,084,257,125,738,940,094,442,196,576,515,467,508,250,307,691,644,831,228,159,149,320,554,050,586,418,335,253,801,049,423,626,
046,725,086,043,977,854,358,317,739,055,430,625,311,862,224,252,362,460,177,015,895,680,900,269,523

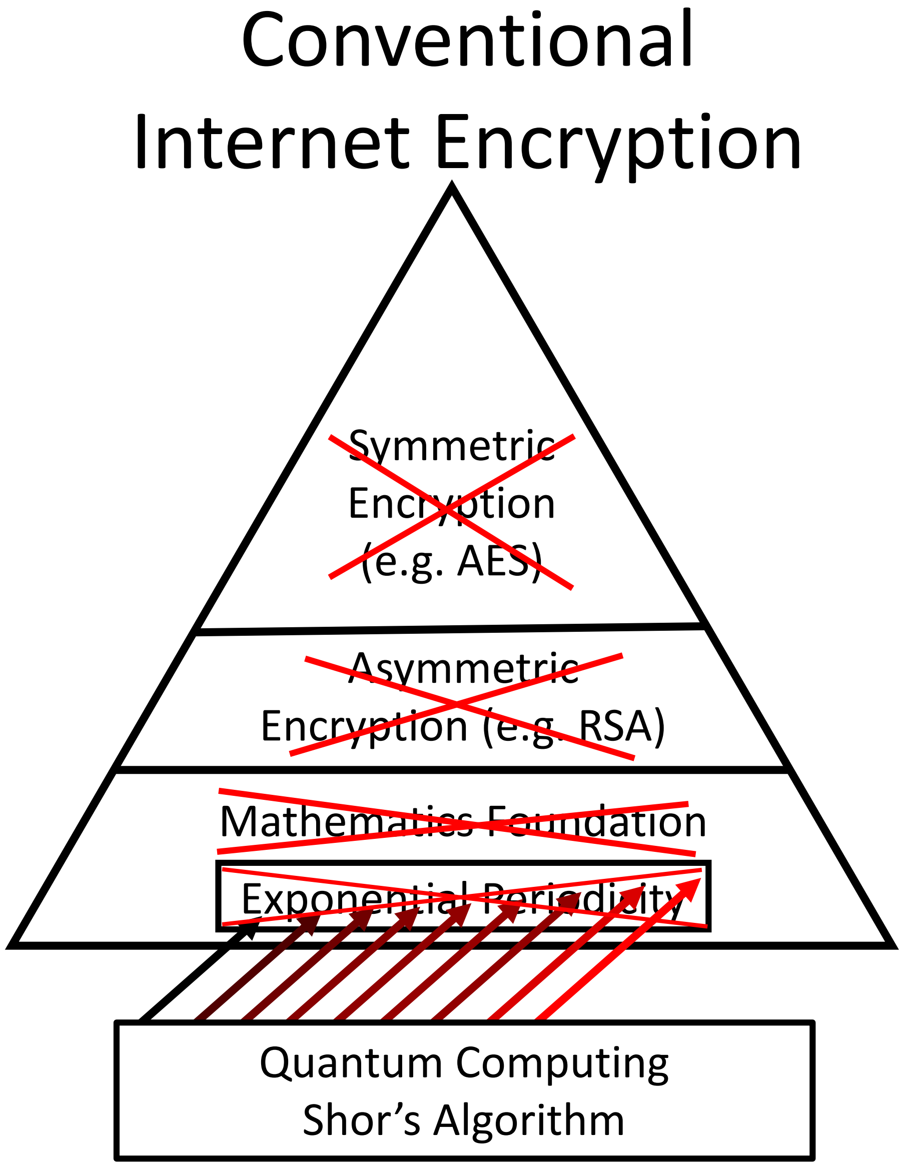
https://www.youtube.com/watch?v=Z8M2BTscoD4&t=10s

What Does Quantum Computing Do?

Quantum Computing Breaks Today’s Asymmetric Key Encryption

$n \Rightarrow p * \mathrm{q}$ factoring	(hours/days/weeks)
$\phi(n) \Rightarrow (p - 1) * (q - 1)$	(*instantly*)
$e \Rightarrow$ Extended Euclid Algorithm $\Rightarrow d$	(*instantly*)
$(m^e)^d \Rightarrow m$	(*instantly*)

What Does Quantum Computing Do?


Conventional
Internet Encryption
~~Symmetric Encryption (e.g. AES)~~
~~Asymmetric Encryption (e.g. RSA)~~
~~Mathematics Foundation~~
~~Exponential Periodicity~~
Quantum Computing
Shor's Algorithm

Mathematics Foundation
is the
Problem

Store Now, Decrypt Later (SNDL)

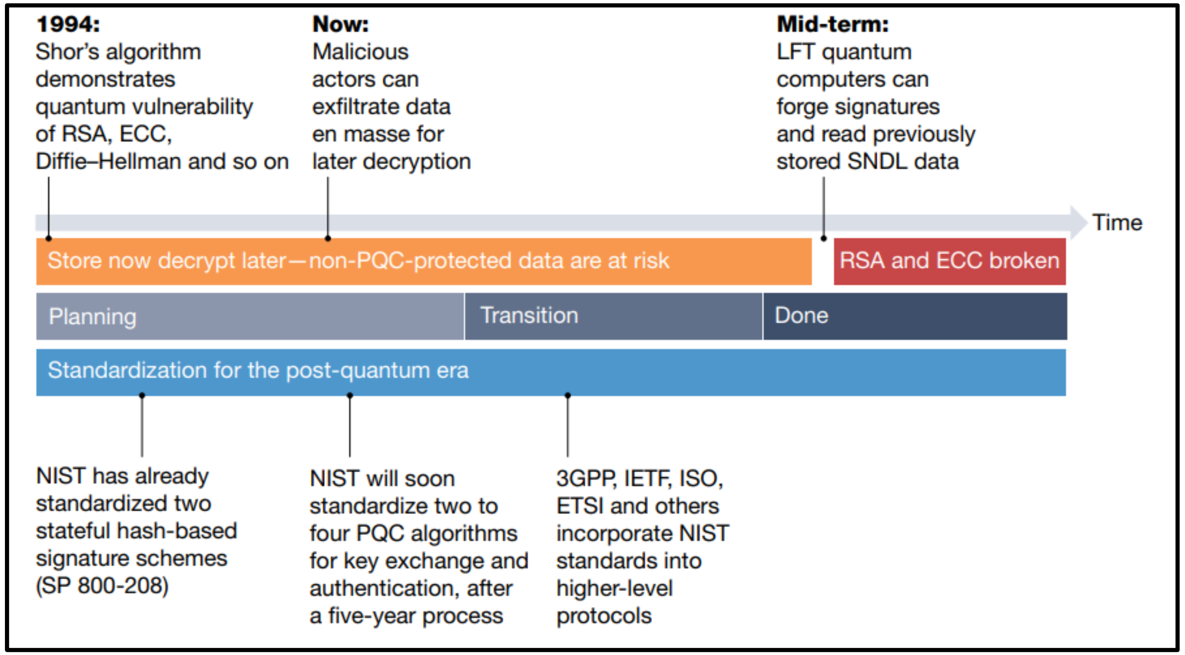
The SNDL attack poses a threat to information that is encrypted now using quantum-vulnerable cryptography. Such encrypted data, which are often transmitted over the public internet infrastructure, can be collected, stored indefinitely and then decrypted in the future once the adversary has access to a LFT [Large and Fault-Tolerant] *quantum computer.*

In some situations, this is not a major concern. However, there are important trade secrets, medical records, national security documents and more that have multidecade shelf lives and must remain confidential for an extended period of time.

For this reason, the SNDL attack is one of the most important arguments to not delay starting the transition any further.

Transitioning organizations to post-quantum cryptography
Nature | Vol 605 | 12 May 2022, Pgs 237-243

Store Now, Decrypt Later



1994:
Shor's algorithm demonstrates quantum vulnerability of RSA, ECC, Diffie–Hellman and so on

Now:
Malicious actors can exfiltrate data en masse for later decryption

Mid-term:
LFT quantum computers can forge signatures and read previously stored SNDL data

Time

Store now decrypt later—non-PQC-protected data are at risk

RSA and ECC broken

Planning

Transition

Done

Standardization for the post-quantum era

NIST has already standardized two stateful hash-based signature schemes (SP 800-208)

NIST will soon standardize two to four PQC algorithms for key exchange and authentication, after a five-year process

3GPP, IETF, ISO, ETSI and others incorporate NIST standards into higher-level protocols

Bumblehive - NSA Utah Data Center, Bluffdale Utah

For those organizations that have not started integrating PQC in their systems or even planning for it, we highly recommend starting their efforts now. Those organizations and enterprises with sensitive data with time value exceeding five years should consider PQC immediately. The SNDL attack is already practicable, so in this context, such organizations are already late and at increasing risk.

Transitioning organizations to post-quantum cryptography
Nature | Vol 605 | 12 May 2022, Pgs 237-243

NICT Post-Quantum Cryptography (PQC) Standardization

… The question of when a large-scale quantum computer will be built is a complicated one. While in the past it was less clear that large quantum computers are a physical possibility, many scientists now believe it to be merely a significant engineering challenge. Some engineers even predict that within the next twenty or so years sufficiently large quantum computers will be built to break essentially all public key schemes currently in use.

Historically, it has taken almost two decades to deploy our modern public key cryptography infrastructure. Therefore, regardless of whether we can estimate the exact time of the arrival of the quantum computing era, we must begin now to prepare our information security systems to be able to resist quantum computing.

NICT Post-Quantum Cryptography (PQC) Standardization

December 2016: NIST's *Call for Proposals* invites participants to submit PQ algorithms for standardization consideration.

By 2018: NIST had received 69 Round 1 algorithms.

In 2019: NIST reduced the algorithms to 26 Round 2 candidates after a series of workshops.

Mid-2020: NIST further reduced the list to seven finalists and eight alternates.

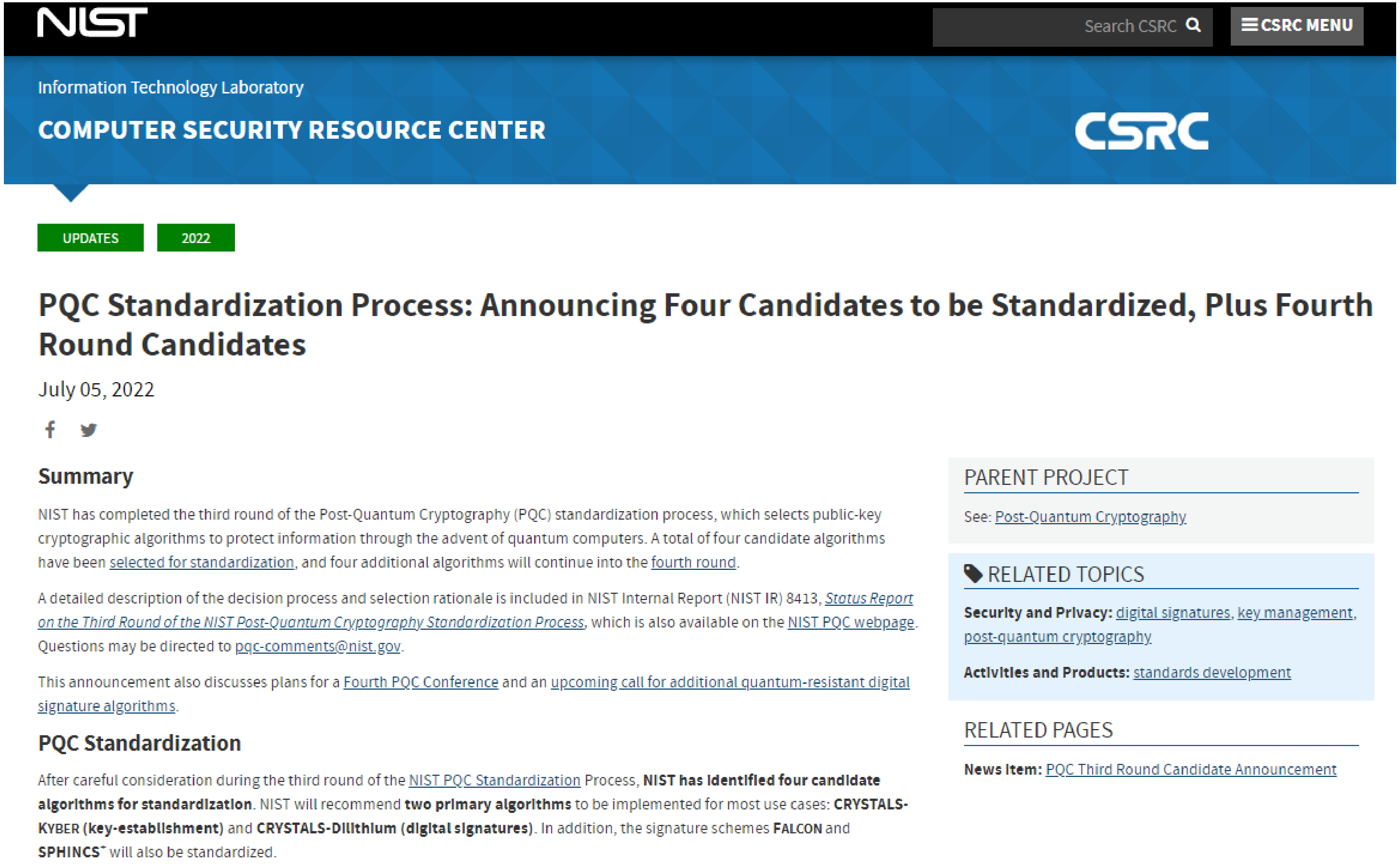
- Public key encryption algorithms
- Digital signature algorithms

No remaining algorithm is suitable for both encryption and signing (unlike RSA).

NIST will select multiple "winners"

- At least one for encryption
- At least one for signing

NICT Post-Quantum Cryptography (PQC) Standardization


NIST
Search CSRC
CSRC MENU
Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER
CSRC
UPDATES
2022

PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates

July 05, 2022

Summary

NIST has completed the third round of the Post-Quantum Cryptography (PQC) standardization process, which selects public-key cryptographic algorithms to protect information through the advent of quantum computers. A total of four candidate algorithms have been selected for standardization, and four additional algorithms will continue into the fourth round.

A detailed description of the decision process and selection rationale is included in NIST Internal Report (NIST IR) 8413, *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*, which is also available on the NIST PQC webpage. Questions may be directed to pqc-comments@nist.gov.

This announcement also discusses plans for a Fourth PQC Conference and an upcoming call for additional quantum-resistant digital signature algorithms.

PQC Standardization

After careful consideration during the third round of the NIST PQC Standardization Process, **NIST has identified four candidate algorithms for standardization**. NIST will recommend **two primary algorithms** to be implemented for most use cases: **CRYSTALS-KYBER (key-establishment)** and **CRYSTALS-Dilithium (digital signatures)**. In addition, the signature schemes **FALCON** and **SPHINCS$^+$** will also be standardized.

PARENT PROJECT

See: Post-Quantum Cryptography

RELATED TOPICS

Security and Privacy: digital signatures, key management, post-quantum cryptography

Activities and Products: standards development

RELATED PAGES

News Item: PQC Third Round Candidate Announcement

Gartner Unveils Top Cybersecurity Predictions for 2022-23

We can’t fall into old habits and try to treat everything the same as we did in the past.

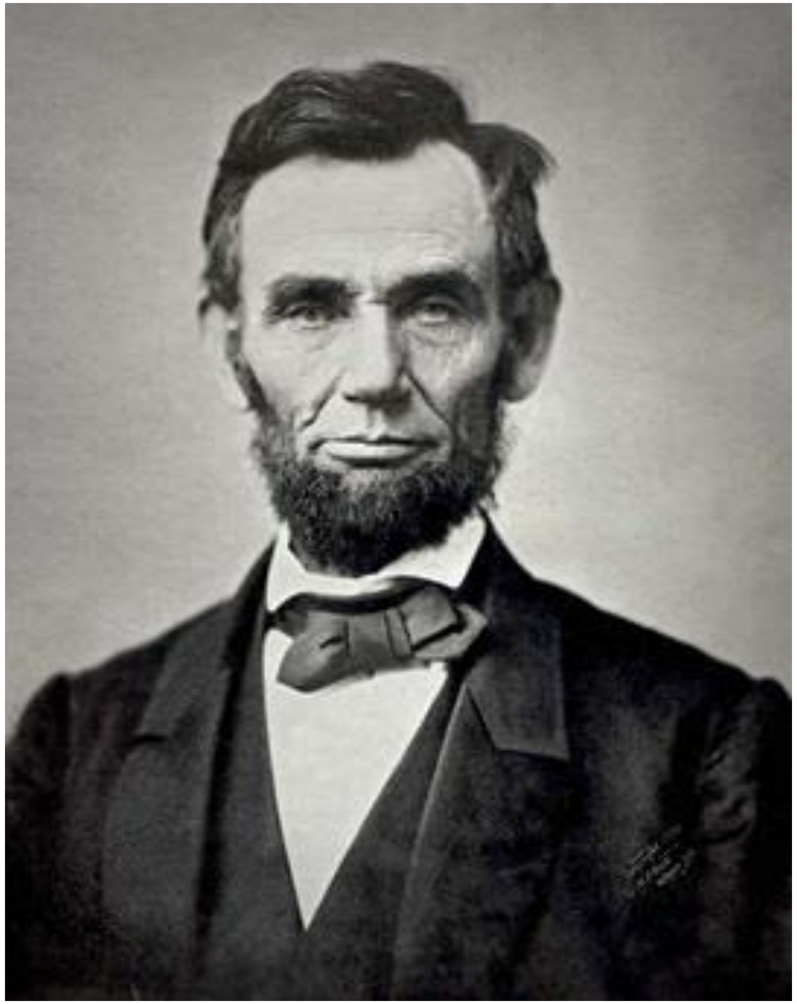
Most security and risk leaders now recognize that major disruption is only one crisis away.

We can’t control it, but we can evolve our thinking, our philosophy, our program and our architecture.

− Richard Addiscott, Gartner Senior Director Analyst.

https://www.gartner.com/en/newsroom/press-releases/2022-06-21-gartner-unveils-the-top-eight-cybersecurity-predictio

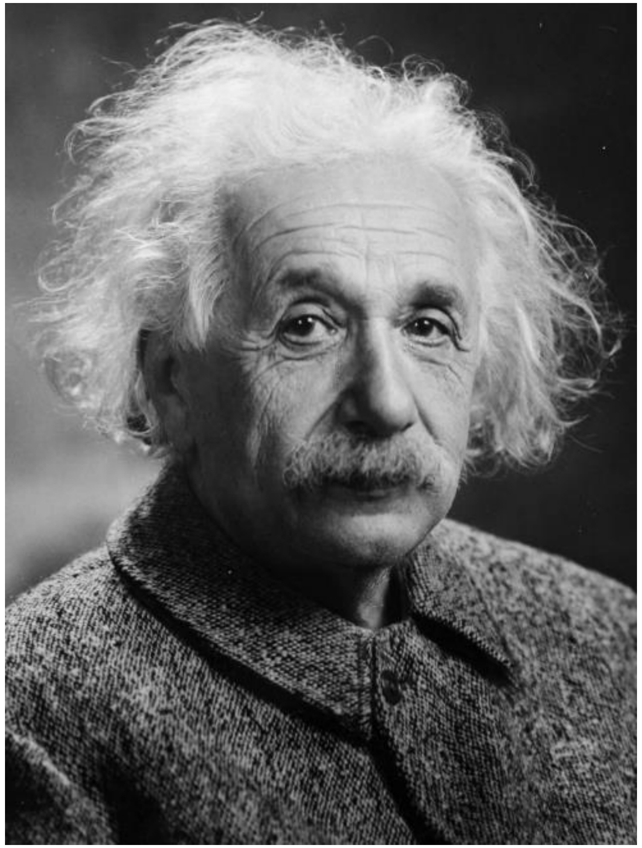
Abraham Lincoln



The dogmas of the quiet past, are inadequate to the stormy present. The occasion is piled high with difficulty, and we must rise -- with the occasion.

As our case is new, so we must think anew, and act anew.

Washington D.C., December 1, 1862

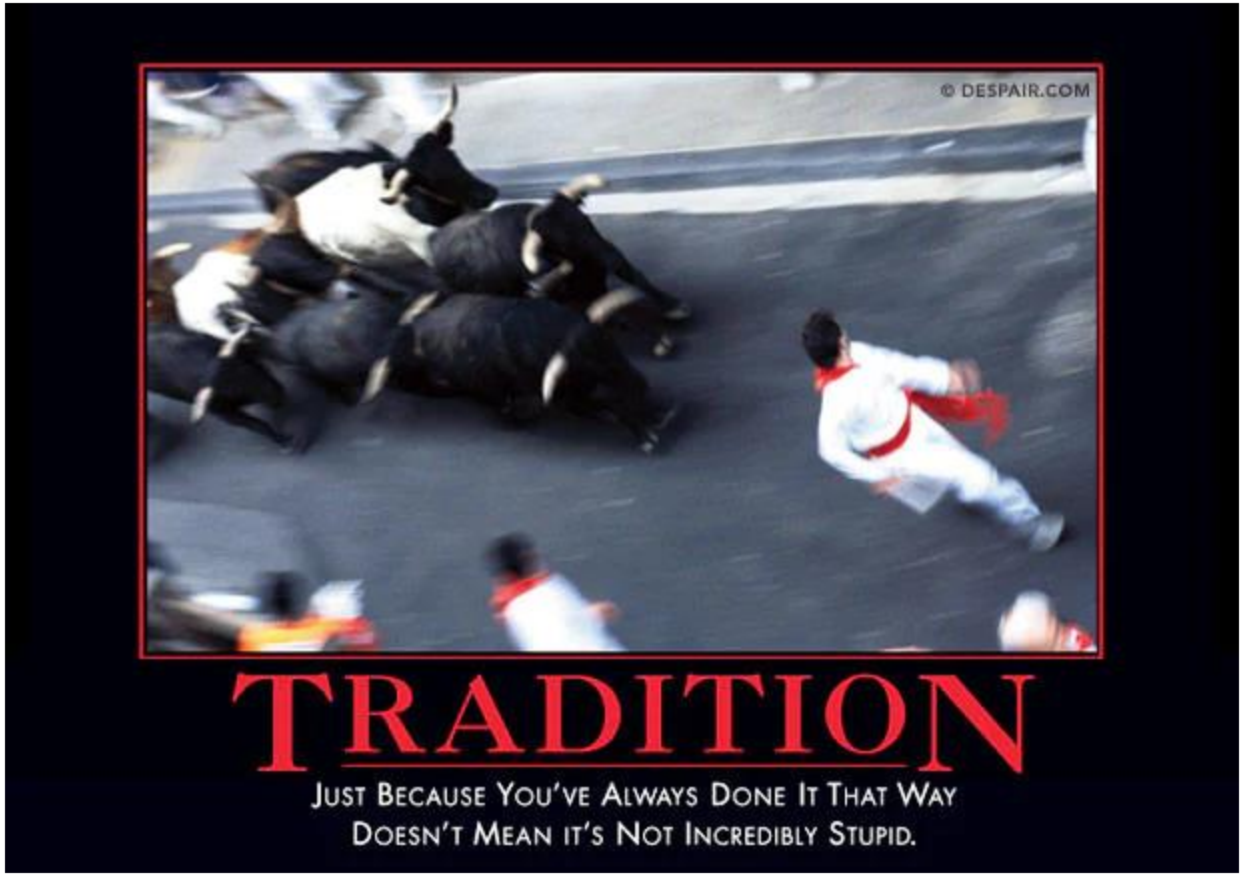


Never said it.

The definition of insanity is doing the same thing over and over again and expecting a different result.

https://commons.wikimedia.org/wiki/Category:Albert_Einstein#/media/File:Albert_Einstein_Head.jpg

Despair.com Demotivation Posters



© DESPAIR.COM
TRADITION
Just Because You've Always Done It That Way
Doesn't Mean It's Not Incredibly Stupid.

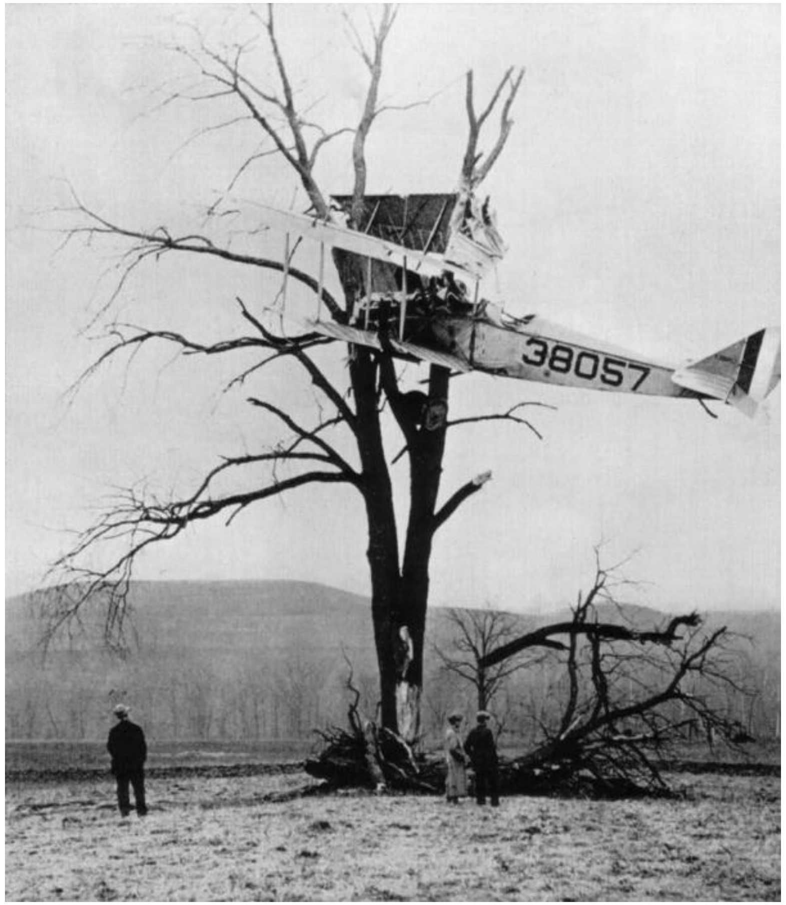
https://despair.com/collections/posters

Gartner Top Cybersecurity Predictions for 2022-23

- Through 2025, 30% of nation states will pass legislation that regulates ransomware payments, fines and negotiations, up from less than 1% in 2021.
- 60% of organizations will embrace Zero Trust as a starting point for security by 2025. More than half will fail to realize the benefits
- By 2025, 60% of organizations will use cybersecurity risk as a primary determinant in conducting third-party transactions and business engagements.
- Through 2023, government regulations requiring organizations to provide consumer privacy rights will cover 5 billion citizens and more than 70% of global GDP.
- By 2025, 70% of CEOs will mandate a culture of organizational resilience to survive coinciding threats from cybercrime, severe weather events, civil unrest and political instabilities.
- By 2025, threat actors will have weaponized operational technology environments successfully to cause human casualties.

https://www.gartner.com/en/newsroom/press-releases/2022-06-21-gartner-unveils-the-top-eight-cybersecurity-predictio

End of Part 1
Thank You



http://www.vlib.us/wwi/resources/archives/images/i050203/images/AMER%23850.jpg

Cybersecurity is inherently difficult. It is terribly unforgiving of any carelessness, incapacity, or neglect.

– With thanks to Captain A. G. Lamplugh
British Aviation Insurance Group

Legal Disclaimer

This presentation is not, and should not be considered,
legal counsel, legal advice, or legal opinion.

Only attorneys should provide legal counsel, legal advice, and legal opinions.
They can be the best friend for $800/hr.

USE THIS PRESENTATION'S INFORMATION AT YOUR OWN RISK.

All presented information represents personal opinions and current understanding.

The presenters do not assume any responsibility or liability for damages
arising from relying on or using this presentation's information.

NO WARRANTIES ARE EXPRESSED OR IMPLIED.

Ransomware in the Era of Quantum Computing
Part 2

W. David Schwaderer
CEO/Co-founder Shape*Shift*™ Ciphers LLC
david@Shape*Shift*Ciphers.com

Speed Bump 1

Moving Target Defense