Research Cybersecurity Landscape in 2022

Von Welch
AVP, Information Security Indiana University
Director, Trusted CI
Director, ResearchSOC

SURA Tech Talk
April 15, 2022

Trusted CI:
The NSF Cybersecurity Center of Excellence

Our mission: to lead in the development of an NSF Cybersecurity Ecosystem with the workforce, knowledge, processes, and cyberinfrastructure that enables trustworthy science and NSF's vision of a nation that is a global leader in research and innovation.

CENTER FOR APPLIED CYBERSECURITY RESEARCH
INDIANA UNIVERSITY
Pervasive Technology Institute

NCSA

BERKELEY LAB

WISCONSIN
UNIVERSITY OF WISCONSIN-MADISON

PITTSBURGH SUPERCOMPUTING CENTER

USA UNIVERSITY OF SOUTH ALABAMA

https://trustedci.org/

ResearchSOC/OmniSOC

- Shared 24x7x365-capable cybersecurity operations center for research & higher education (R&E).
- Average volume across all members: > 9.4 TB/day; > 14.2 B events/day; > 162k EPS.
- Provides higher ed/research-focused virtual cybersecurity services:
  - CISO, CISO advisory, partial FTE security staff, specialized incident response teams.
- Elastic is key technology partner.
- Members: US ARF, CWRU, Clemson, Creighton, GAGE, Gemini, I-Light, IU, Lehigh, U. Nebraska, Northwestern U., NRAO, NSO Rutgers U., Santa Clara U., SOX

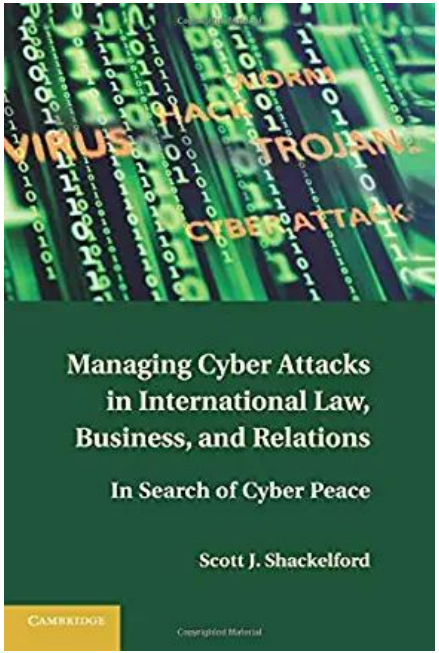
My Talk


NSF
Image credit: Pixabay https://www.pexels.com/photo/black-textile-41949/

International Cyber Conflicts

Some notable incidents…

- 1982 Soviet gas pipeline
- 1999 NATO web DDOS
- 2001 Moonlight Maze
- 2003 Titan Rain
- 2007 Estonia
- 2008 Georgia
- 2009 Operation Aurora
- 2010 Stuxnet
- 2017 WannaCry
- 2018 NotPetya

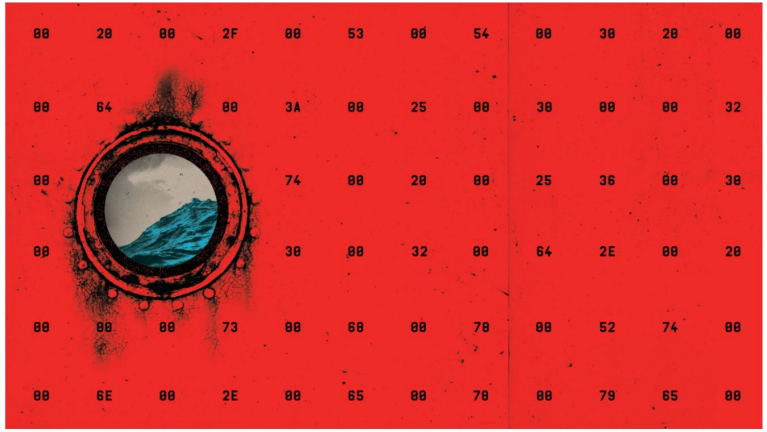


Potential Global Impact of Cyberconflict

ANDY GREENBERG | EXCERPT | SECURITY | AUG 22, 2018 5:00 AM

The Untold Story of NotPetya, the Most Devastating Cyberattack in History

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.



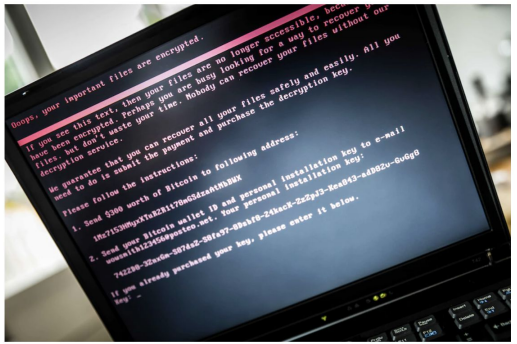
MIKE MCQUADE

National Security

Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes

By Ellen Nakashima

January 12, 2018



A laptop displays a message after it was infected with ransomware resembling the 'NotPetya' attack last year. (Rob Engelaar/EPA)

The CIA has attributed to Russian military hackers a cyberattack that crippled computers in Ukraine last year, an effort to disrupt that country's financial system amid its ongoing war with separatists loyal to the Kremlin.

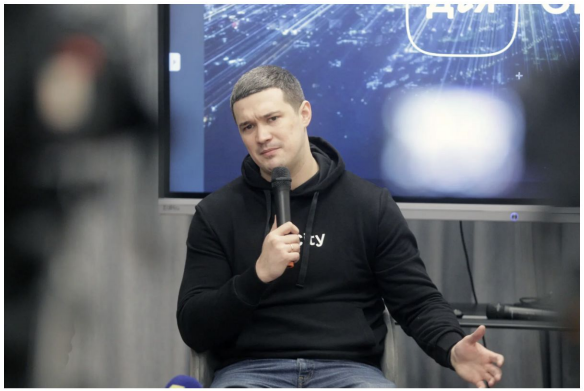
https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html

The Democratization of Cyberattacks

Volunteer Hackers Converge on Ukraine Conflict With No One in Charge

The hackers have claimed a number of disruptions over the past week, blurring the lines between amateurs and groups linked to governments.

288



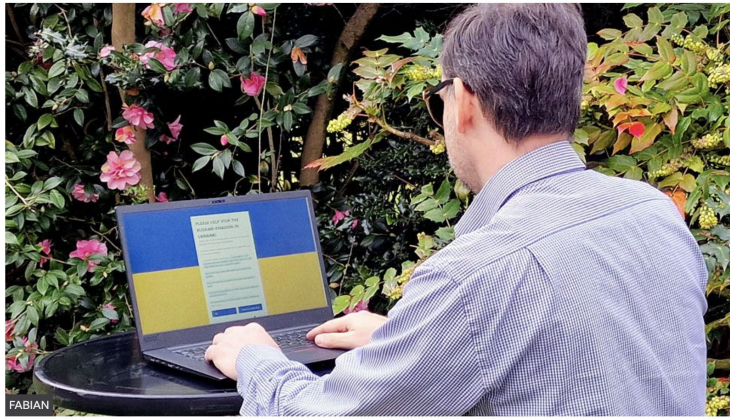
Mykhailo Fedorov, Ukraine's minister of digital transformation, in December. "We are creating an I.T. army," he tweeted on Saturday. Yevhen Kotenko/Ukrinform, via Getty Images

Ukraine: Spam website set up to reach millions of Russians

By Joe Tidy
Cyber reporter

3 days ago

Russia-Ukraine war



Fabian at work on his spamming website

A Norwegian computer expert has created a website enabling anyone to send an email about the war in Ukraine to up to 150 Russian email addresses at a time, so that Russian people have a chance to hear the truth their government is hiding.

As Tanks Rolled Into Ukraine, So Did Malware. Then Microsoft Entered the War.

After years of talks about the need for public-private partnerships to combat cyberattacks, the war in Ukraine is stress-testing the system.

157

Ukrainians gather in a train station in Kyiv in an effort to leave the city shortly after the Russian invasion began. Lynsey Addario for The New York Times

By David E. Sanger, Julian E. Barnes and Kate Conger

https://www.nytimes.com/2022/03/04/technology/ukraine-russia-hackers.html - https://www.bbc.com/news/technology-60697261 - https://www.nytimes.com/2022/02/28/us/politics/ukraine-russia-microsoft.html

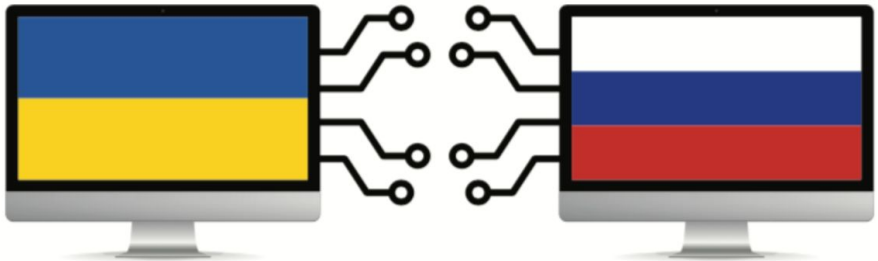
KrebsonSecurity
In-depth security news and investigation

HOME ABOUT THE AUTHOR ADVERTISING/SPEAKING

Report: Recent 10x Increase in Cyberattacks on Ukraine

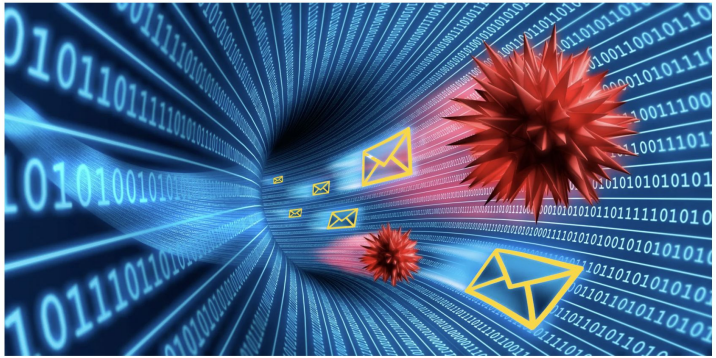
March 11, 2022 13 Comments

As their cities suffered more intense bombardment by Russian military forces this week, Ukrainian Internet users came under renewed cyberattacks, with one Internet company providing service there saying they blocked ten times the normal number of phishing and malware attacks targeting Ukrainians.



Fake antivirus updates used to deploy Cobalt Strike in Ukraine

By Bill Toulas March 14, 2022 05:52 PM 0



Ukraine's Computer Emergency Response Team is warning that threat actors are distributing fake Windows antivirus updates that install Cobalt Strike and other malware.

https://krebsonsecurity.com/2022/03/report-recent-10x-increase-in-cyberattacks-on-ukraine/ - https://www.bleepingcomputer.com/news/security/fake-antivirus-updates-used-to-deploy-cobalt-strike-in-ukraine/

Balkanization

With the escalating situation in Ukraine and the increased threat of cyber attacks from Russia, its allies, as well as the countries Russia has compromised within cyberspace, it is recommended the network traffic to and from the following countries be blocked using the GeoIP filter/blocking feature on your edge devices (i.e. firewalls, proxy filters, etc.) where appropriate.

Geo-blocking traffic will help reduce your organization's overall attack surface. Furthermore, it is recommended that any additional countries with which you currently do not, or expect to have legitimate interactions with in the future, be blocked using this feature as well.

Recommended countries to block:

- Russia
- Iran
- Ukraine
- North Korea
- China
- Turkey
- Belarus
- Venezuela
- Netherlands

Internet Backbone Giant Lumen Shuns .RU

March 8, 2022 45 Comments

Lumen Technologies, an American company that operates one of the largest Internet backbones and carries a significant percentage of the world's Internet traffic, said today it will stop routing traffic for organizations based in Russia. Lumen's decision comes just days after a similar exit by backbone provider **Cogent**, and amid a news media crackdown in Russia that has already left millions of Russians in the dark about what is really going on with their president's war in Ukraine.

Russia, Blocked From the Global Internet, Plunges Into Digital Isolation

Russian authorities and multinational companies have erected a digital barricade between the country and the West, erasing the last remnants of independent information online.

https://www.nytimes.com/2022/03/07/technology/russia-ukraine-internet-isolation.html
https://krebsonsecurity.com/2022/03/internet-backbone-giant-lumen-shuns-ru/

Supply Chain Concerns

March 31, 2022
6:05 PM EDT
Last Updated 7 days ago

Disrupted

EXCLUSIVE U.S. warned firms about Russia's Kaspersky software day after invasion -sources

By Christopher Bing

4 minute read

https://www.reuters.com/technology/exclusive-us-warned-firms-about-russias-kaspersky-software-day-after-invasion-2022-03-31/

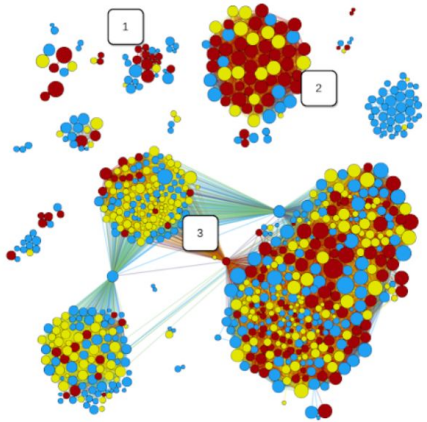
Suspicious Twitter Activity around the Russian Invasion of Ukraine

< Return to Blog Listing

March 10, 2022

On February 24, 2022, Russia began a full-scale military invasion of Ukraine. The global scale of national interests related to the invasion means that public opinion in many countries is likely to play a significant role in the conflict. In turn, social media can play a key role in shaping public opinion in geopolitical events. Consequently, the potential to exploit social vulnerabilities through social media is of great concern. Detecting and monitoring these kinds of abuse is part of our mission at the Observatory on Social Media.

In collaboration with the Polytechnic University of Milan, we compiled a list of almost 40 English, German, Russian, and Ukrainian keywords relevant to the invasion and used them to collect over 60 million tweets posted since February 1. In our white paper *Suspicious Twitter Activity around the Russian Invasion of Ukraine* we present some preliminary evidence of suspicious activity obtained from analysis of this data. We report on a dramatic spike in the creation of new accounts around the date of the invasion, and on several networks of accounts sharing suspiciously similar content.



https://osome.iu.edu/research/blog/suspicious-twitter-activity-around-the-russian-invasion-of-ukraine

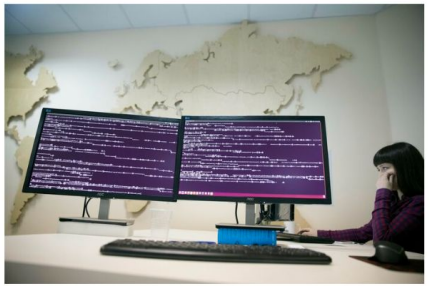
Feature

Russia War Raises Global Insurers' Cyber Claim Exposure

By **Daphne Zhang** · Listen to article

Law360 (March 11, 2022, 4:30 PM EST) -- Global insurers are on high alert for an increase in cyberattack and business interruption claims as a result of Russia's invasion of Ukraine, facing growing exposure as the networks of Ukraine and its Western allied countries' critical infrastructure sectors are attacked and threatened.

Ukraine's critical infrastructure, government services, banks and telecom sectors have already been hit with cyberattacks since late February. Amid rising military and diplomatic support from the United States, United Kingdom, European Union and Japan, the chance of a systemic cyberattack spillover to those countries is "only a matter of time," according to cybersecurity and insurance experts.



The possibility of a Russia-related widespread cyberattack in the wake of the country's invasion of Ukraine is making insurers anxious, especially given a recent New Jersey court ruling that a warlike exclusion does not bar coverage to cyberwars, a data security tech executive said. (AP Photo/Pavel Golovkin)

"This is probably the first true war being fought in a pretty active cyber environment," said Sridhar Manyem, director of industry research and analytics at AM Best. "There are a lot of activists from both sides of Ukraine and Russia trying to engage in this cyber warfare. Therefore, threats have escalated in an already active environment."

Useful Tools & Links

Add to Briefcase
Save to PDF & Print
Rights/Reprints
Editorial Contacts

Related Sections

Aerospace & Defense
Banking
Corporate
Corporate Crime & Compliance UK
Cybersecurity & Privacy
Energy
Insurance
Insurance UK
Telecommunications

Law Firms

Morrison & Foerster

Companies

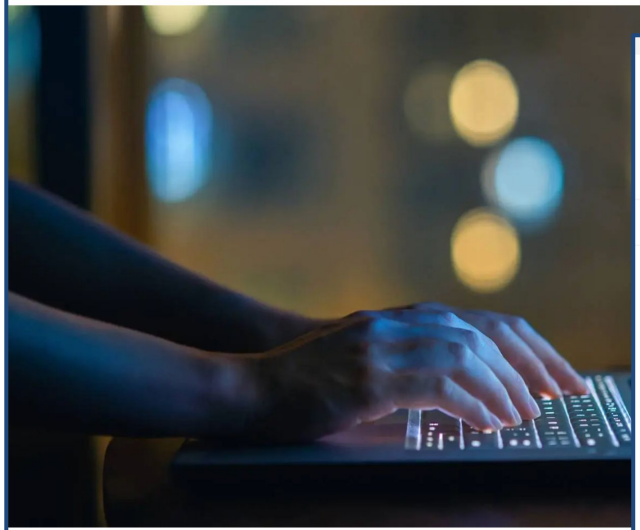
Aon PLC
AXA SA
CNA Financial Corp.
GuidePoint Security LLC
Merck & Co. Inc.

Government Agencies

European Union
Office of Foreign Assets Control

CYBERSECURITY HIGHER EDUCATION

'Everyone' must prepare for university cyberattacks, says FBI agent



(Getty Images)

Written by Emily Bamforth

MAR 9, 2022 | EDSCOOP

"Everyone" should be involved in preparations for cyberattacks, including senior university leaders who lack technical expertise, speakers said during a virtual event Wednesday hosted by the University of California.

An official website of the United States government Here's how you know

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Search

CISA.gov Services Report

Alerts and Tips Resources Industrial Control Systems

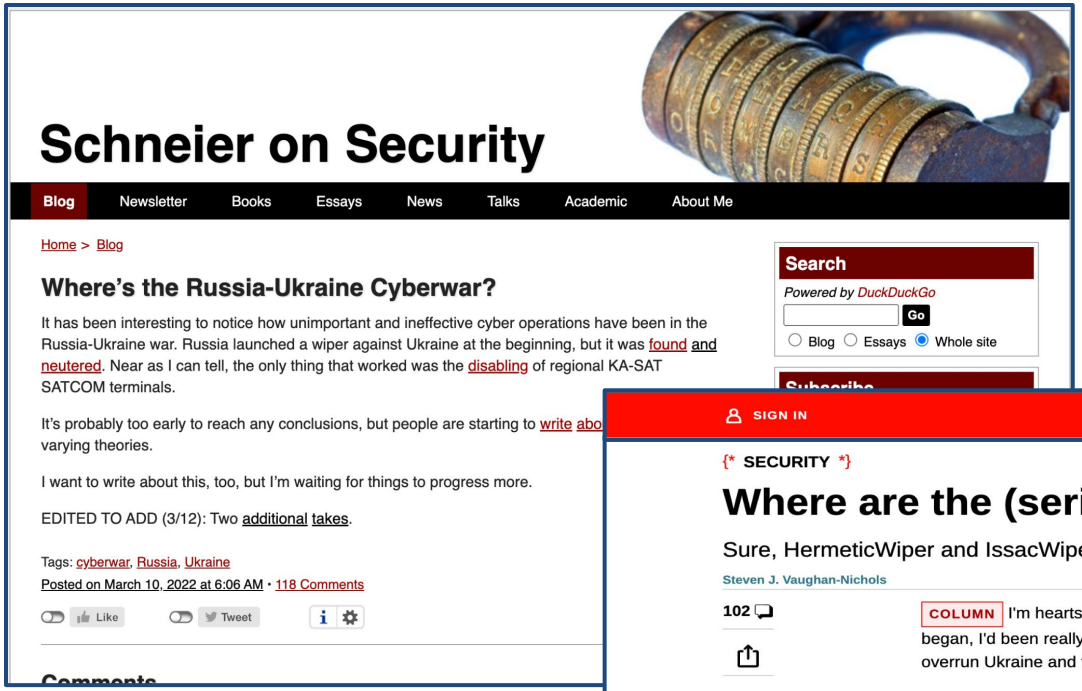
Russia Cyber Threat Overview and Advisories

This page provides an overview of the Cybersecurity and Infrastructure Security Agency's (CISA's) assessment of the Russian government's malicious cyber activities. The overview leverages publicly available, open-source intelligence and information regarding this threat. This page also includes a complete list of related CISA publications, many of which are jointly authored with other U.S. government agencies (Note: unless specifically stated, neither CISA nor the U.S. Government attributed specific activity described in the referenced sources to Russian government actors). Additionally, this page provides instructions on how to report related threat activity.

The Russian government engages in malicious cyber activities to enable broad-scope cyber espionage, to suppress certain social and political activity, to steal intellectual property, and to harm regional and international adversaries.[1] Recent Advisories published by CISA and other unclassified sources reveal that Russian state-sponsored threat actors are targeting the following industries and organizations in the United States and other Western nations: COVID-19 research, governments, election organizations, healthcare and pharmaceutical, defense, energy, video gaming, nuclear, commercial facilities, water, aviation, and critical manufacturing. The same reporting associated Russian actors with a range of high-profile malicious cyber activity, including the 2020 compromise of the SolarWinds software supply chain, the 2020 targeting of U.S. companies developing COVID-19 vaccines, the 2018 targeting of U.S industrial control system infrastructure, the 2017 NotPetya ransomware attack on organizations worldwide, and the 2016 leaks of documents stolen from the U.S. Democratic National Committee.

According to the U.S. Office of the Director of National Intelligence 2021 Annual Threat Assessment, "Russia continues to target critical infrastructure, including underwater cables and industrial control systems, in the United States and in allied and partner countries, as compromising such infrastructure improves—and in some cases can demonstrate—its ability to damage infrastructure during a crisis." The Assessment states that "Russia almost certainly considers cyber attacks an acceptable option to deter adversaries, control escalation, and prosecute conflicts."[2]

https://edscoop.com/university-cyberattacks-fbi-response/
https://www.cisa.gov/uscert/russia



Schneier on Security

Blog | Newsletter | Books | Essays | News | Talks | Academic | About Me

Home > Blog

Where's the Russia-Ukraine Cyberwar?

It has been interesting to notice how unimportant and ineffective cyber operations have been in the Russia-Ukraine war. Russia launched a wiper against Ukraine at the beginning, but it was found and neutered. Near as I can tell, the only thing that worked was the disabling of regional KA-SAT SATCOM terminals.

It's probably too early to reach any conclusions, but people are starting to write abo
varying theories.

I want to write about this, too, but I'm waiting for things to progress more.

EDITED TO ADD (3/12): Two additional takes.

Tags: cyberwar, Russia, Ukraine

Posted on March 10, 2022 at 6:06 AM • 118 Comments

Like Tweet

Search

Powered by DuckDuckGo

Go

Blog Essays Whole site

Subscribe

SIGN IN The Register

{* SECURITY *}

Where are the (serious) Russian cyberattacks?

Sure, HermeticWiper and IssacWiper are bad, but they're not BAD in capital letters

Steven J. Vaughan-Nichols

Wed 9 Mar 2022 // 10:29 UTC

102

COLUMN I'm heartsick over Russia's invasion of Ukraine. But, before it began, I'd been really worried about Russian cyberattacks, which would overrun Ukraine and flood into the West's infrastructure.

I foresaw the Russian GRU Sandworm hacking group launching a cyber attack that would ruin the European Union's power grid or wreck major US internet sites such as Google, Facebook, and Microsoft – or stop cellular services in their tracks.

I was wrong. So far, anyway.

Oh certainly HermeticWiper and IssacWiper – which will wipe all your data and your software and operating system for good measure – will ruin your day, but even together neither will make whole companies or countries miserable. And, to no-one's surprise Russia and its puppets have launched Distributed Denial of Service (DDoS) attacks on Ukrainian sites.

https://www.schneier.com/blog/archives/2022/03/wheres-the-russia-ukraine-cyberwar.html
https://www.theregister.com/2022/03/09/where_are_the_russian_cyberattacks/

CERN Accelerating science

ABOUT NEWS SCIENCE

News › News › Topic: Computing

Voir en français

Computer Security: Vigilance and calmness

24 FEBRUARY, 2022 | By Computer Security team

(Image: CERN)

https://home.cern/news/news/computing/computer-security-vigilance-and-calmness

The Register

{* SECURITY *}

China APT group using Russia invasion, COVID-19 in phishing attacks

Mustang Panda deploys variant of Korplug malware to target European officials and ISPs

Jeff Burt Mon 28 Mar 2022 // 16:30 UTC

A China-based threat group is likely running a month-long campaign using a variant of the Korplug malware and targeting European diplomats, internet service providers (ISPs) and research institutions via phishing lures that refer to Russia's invasion of Ukraine and COVID-19 travel restrictions.

The ongoing campaign was first seen in August 2021 and is being tied to Mustang Panda – a Chinese APT unit also known as TA416, RedDelta and PKPLUG – due to similar code and common tactics, techniques and procedures used by the group in the past, according to researchers with the cybersecurity firm ESET.

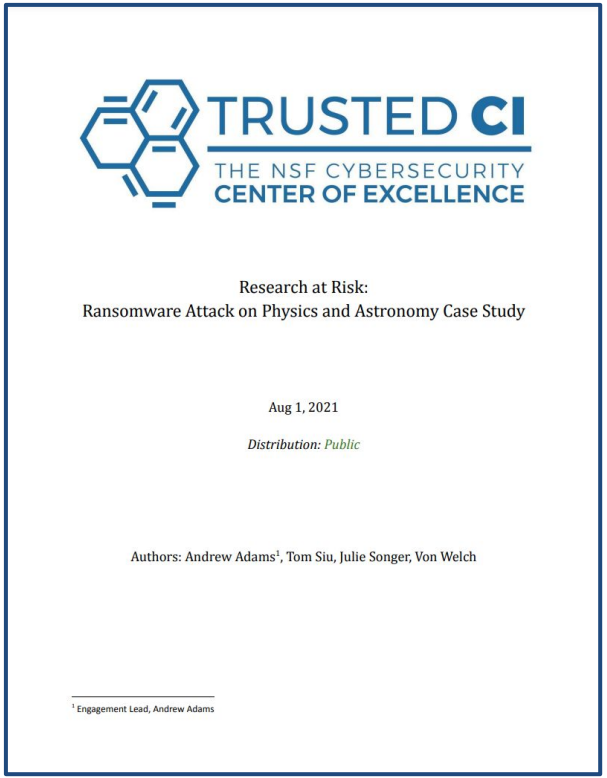
https://www.theregister.com/2022/03/28/mustang-panda-korplug-variant/

Growing Ransomware Risk to Science

Ransomware has changed the cybercrime landscape, broadly expanding potential victims to include hospitals, schools, cities, and researchers.

Trusted CI Collaboration with Michigan State University office of the CIO to document impact of ransomware attack on research.

Report available at:
https://hdl.handle.net/2022/26638


TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Research at Risk:
Ransomware Attack on Physics and Astronomy Case Study

Aug 1, 2021

Distribution: Public

Authors: Andrew Adams[1], Tom Siu, Julie Songer, Von Welch

[1] Engagement Lead, Andrew Adams

My Talk


Image credit: Pixabay https://www.pexels.com/photo/black-textile-41949/

Cybersecurity Maturity Model Certification 2.0: What It Means for Higher Education

Mike Corn Tuesday, December 14, 2021 Cybersecurity and Privacy

6 min read

The first iteration of the Cybersecurity Maturity Model Certification program (CMMC 1.0) approached cybersecurity as an abstract set of rules that were largely removed from how security is practiced. The changes in CMMC 2.0 seem to be a direct response to the weaknesses of CMMC 1.0.

Credit: vs148 / Shutterstock.com © 2021

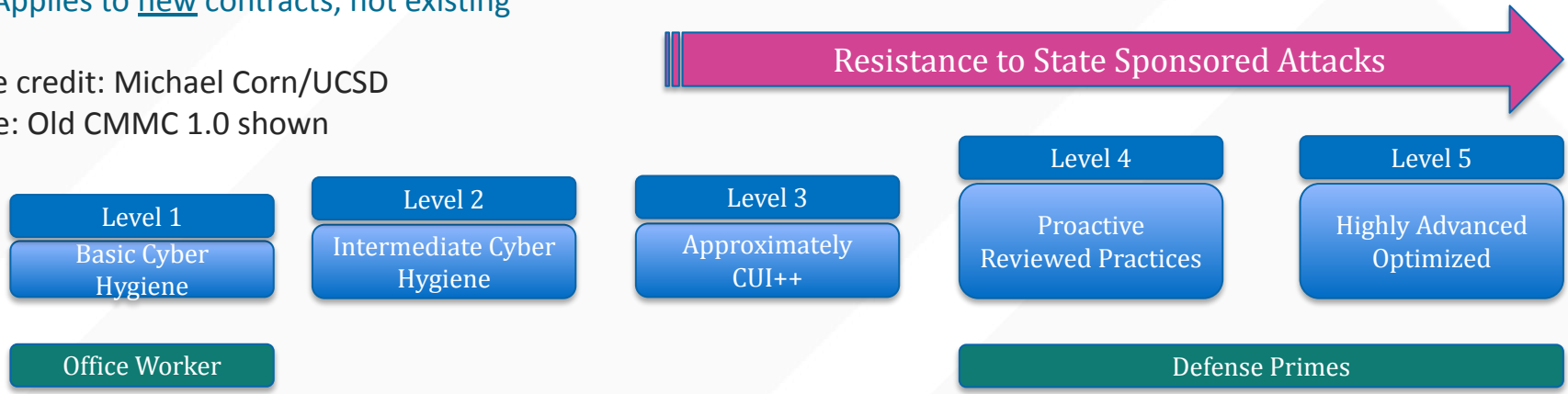
https://er.educause.edu/articles/2021/12/cybersecurity-maturity-model-certification-2-0-what-it-means-for-higher-education

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) TRUST, BUT VERIFY

- New addition to the Defense Federal Acquisition Regulation Supplement (DFARS)
- Adds a verification step to compliance with contractually obligated security practices
- Requires pre-certification of an environment before proposal award
- Applies to new contracts, not existing

- Five tier system of security and IT practices
- Each tier represents an increasing level of maturity of practices
- Level 3 is very challenging to meet and requires a major change in research IT operations – primary focus for most campuses – including UC San Diego

Slide credit: Michael Corn/UCSD
Note: Old CMMC 1.0 shown



HIGHER EDUCATION VS. DEFENSE IND. BASE

Higher Education

- Core mission: education, research, public service (non-profit)
- Open, peer reviewed science
- Integrated teaching/research environments
- Highly decentralized administrative and research environments
- Fundamentally collaborative

Defense Industrial Base (DiB)

- Profit motive
- Closed, intellectual property
- Restricted staff and personnel
- Project / product focused
- Centralized span of control

Credit: Michael Corn / UCSD

COMMENTARY

Let the dust settle on CMMC 2.0

Johann Dettweiler
January 13, 2022 1:17 pm 3 min read

For the past several months, there has been a frantic scrambling by all stakeholders involved in the Cybersecurity Maturity Model Certification (CMMC) program — the Accreditati Department, the third-party assessment organizations (C3PAO) and defense indu to determine the best path forward to secure the nation's supply chain. This was the beginning. The problem was that the program was never really thought throu implement the requirements, the requirements themselves kept changing, and bo up toward implementing what did seem to be settled.

Then on Nov. 4, DoD released a new document, "48 CFR Chapter 2 — Cybersecur Certification (CMMC) 2.0 Updates and Way Forward,"that outlined some monun program. DoD also updated its CMMC reference website to include new details c like. I urge everyone to go to the website and take a look.

At a high level, here are the important takeaways from CMMC 2.0:

- There are now going to be three levels of security, reduced from CMMC 1.0's f

CYBERSECURITY

More companies may have to get a CMMC assessment after all

Justin Doubleday | @jdoubledayWFED
February 10, 2022 6:42 pm 4 min read

More companies may have to get a CMMC assessment after all

00:00:00

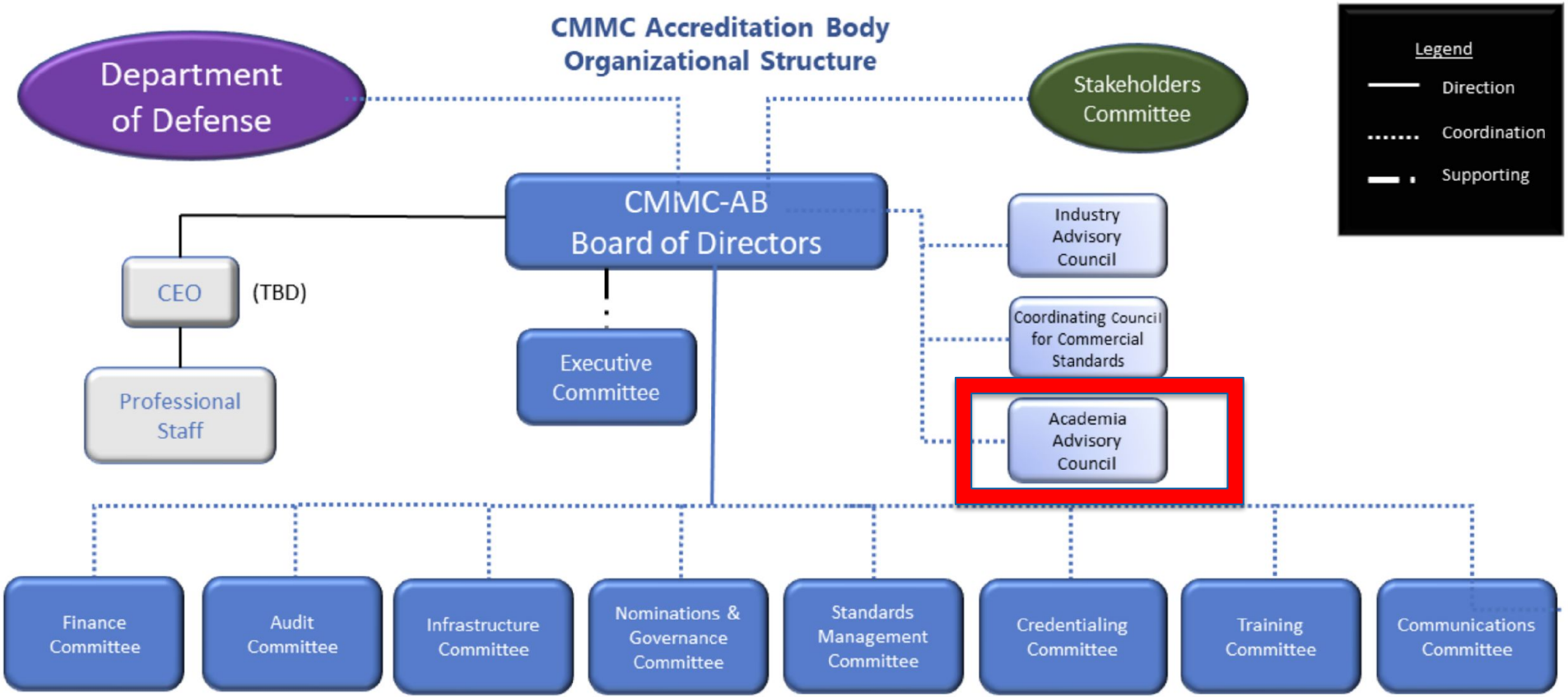
The Pentagon's revamped Cybersecurity Maturity Model Certification program is moving forward under the Defense Department chief information officer, but DoD is rolling back an aspect of the plan that would have allowed some 40,000 companies to self-attest to their cybersecurity practices.

When the Pentagon initially announced the "CMMC 2.0" changes late last year, DoD planned on "bifurcating" requirements for the approximately 80,000 contractors that handle controlled unclassified information (CUI).

At the time, officials said only half of those 80,000 manage CUI that is truly sensitive if it were to fall into the hands of U.S. adversaries. While those contractors would still be required to get a third-party assessment, officials anticipated the other 40,000 managing less risky data would only need to submit a self-assessment.

But during a Feb. 10 town hall, Deputy DoD CIO David McKeown said further analysis has shown all 80,000 will require third-party assessments.

https://federalnewsnetwork.com/commentary/2022/01/let-the-dust-settle-on-cmmc-2-0/
https://federalnewsnetwork.com/cybersecurity/2022/02/more-companies-may-have-to-get-a-cmmc-assessment-after-all/


CMMC Accreditation Body
Organizational Structure
Department of Defense
Stakeholders Committee
Legend
Direction
Coordination
Supporting
CMMC-AB Board of Directors
CEO
(TBD)
Professional Staff
Executive Committee
Industry Advisory Council
Coordinating Council for Commercial Standards
Academia Advisory Council
Finance Committee
Audit Committee
Infrastructure Committee
Nominations & Governance Committee
Standards Management Committee
Credentialing Committee
Training Committee
Communications Committee

APS Encouraged by New Guidance for NSPM-33 Implementation

January 21, 2022

The American Physical Society (APS) is encouraged by the Biden Administration's recently published implementation guidance for National Security Presidential Memorandum 33 (NSPM-33). The guidance—published as a report by the National Science and Technology Council Subcommittee on Research Security of the Joint Committee on the Research Environment—provides the federal science agencies direction on key areas of research security.

The report contains several guidance provisions for agencies that are aligned with APS recommendations that have been central to the Society's advocacy efforts. These include: establishing standardized disclosure requirements for researchers across agencies; providing a pathway to enable researchers to correct past disclosure mistakes; and involving the Department of Justice only "when warranted." Additionally, the guidance document explicitly requires that "Agencies must implement NSPM-33 provisions and related requirements in a nondiscriminatory manner that does not stigmatize or treat unfairly members of the research community, including members of ethnic or racial minority groups."

APS will continue to work with the Biden Administration to help ensure that the United States maintains an environment for fundamental research that is both open and secure and continues to be a destination of choice for global talent.

The full guidance is available on the White House website.

https://www.aps.org/policy/analysis/new-guidance.cfm

NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

GUIDANCE FOR IMPLEMENTING NATIONAL SECURITY PRESIDENTIAL MEMORANDUM 33 (NSPM-33) ON NATIONAL SECURITY STRATEGY FOR UNITED STATES GOVERNMENT-SUPPORTED RESEARCH AND DEVELOPMENT

A Report by the

Subcommittee on Research Security

Joint Committee on the Research Environment

January 2022

6. Ensuring that cybersecurity elements of research security programs meet the objectives of the requirement

6. Ensuring that cybersecurity elements of research security programs meet the objectives of the requirement

Agencies should require that research organizations satisfy the cybersecurity element of the research security program requirement by applying the following basic safeguarding protocols and procedures:

- Provide regular cybersecurity awareness training for authorized users of information systems, including in recognizing and responding to social engineering threats and cyber breaches.
- Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
- Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
- Verify and control/limit connections to and use of external information systems.
- Control any non-public information posted or processed on publicly accessible information systems.
- Identify information system users, processes acting on behalf of users, or devices.
- Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
- Monitor, control, and protect organizational communications (*i.e.*, information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
- Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
- Provide protection of scientific data from ransomware and other data integrity attack mechanisms.
- Identify, report, and correct information and information system flaws in a timely manner.
- Provide protection from malicious code at appropriate locations within organizational information systems.
- Update malicious code protection mechanisms when new releases are available.
- Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

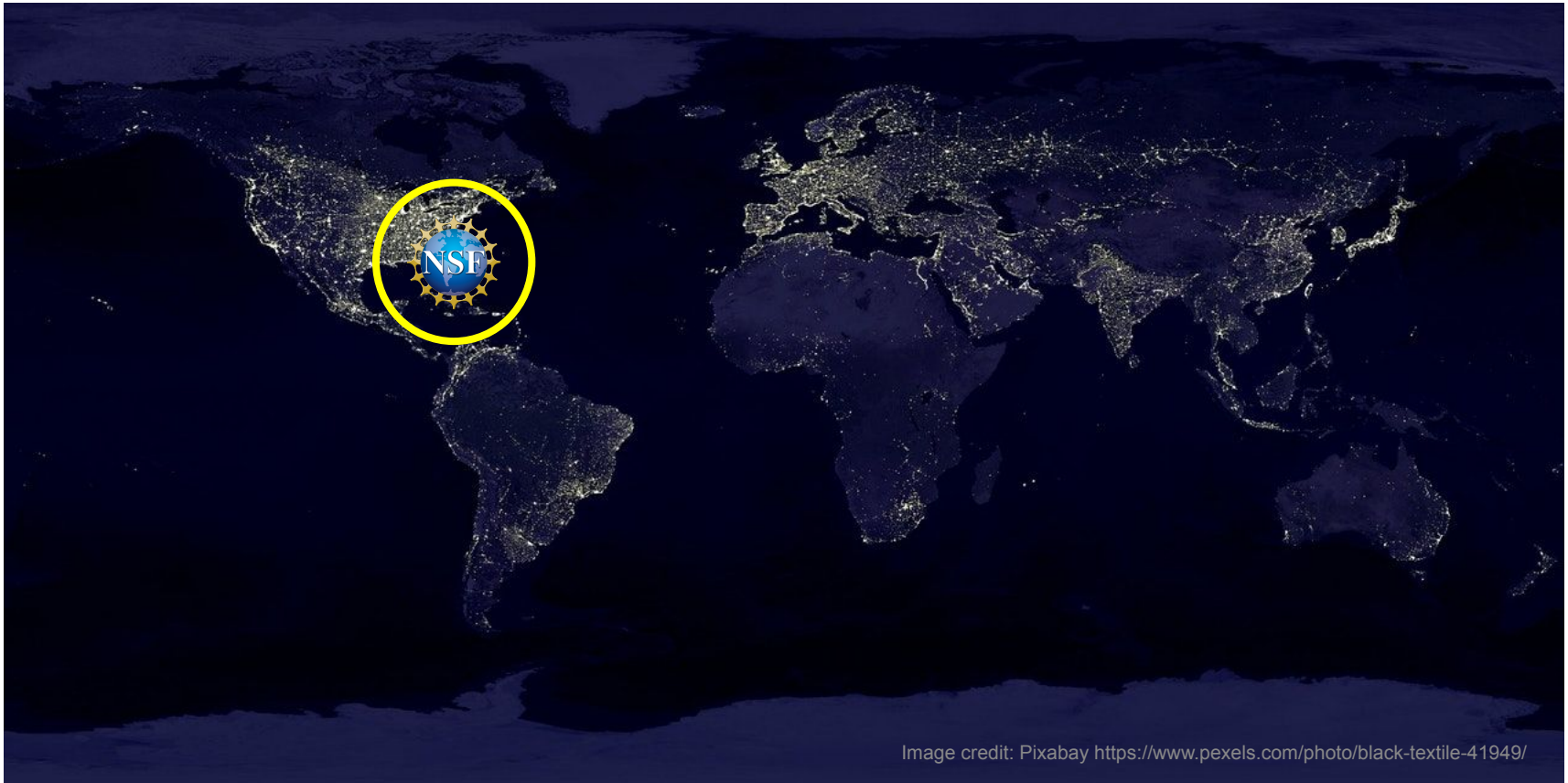
Additional cybersecurity requirements, for example, those provided by the National Institute of Standards and Technology (NIST), will apply in some cases, such as for research involving classified information or CUI.

https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf

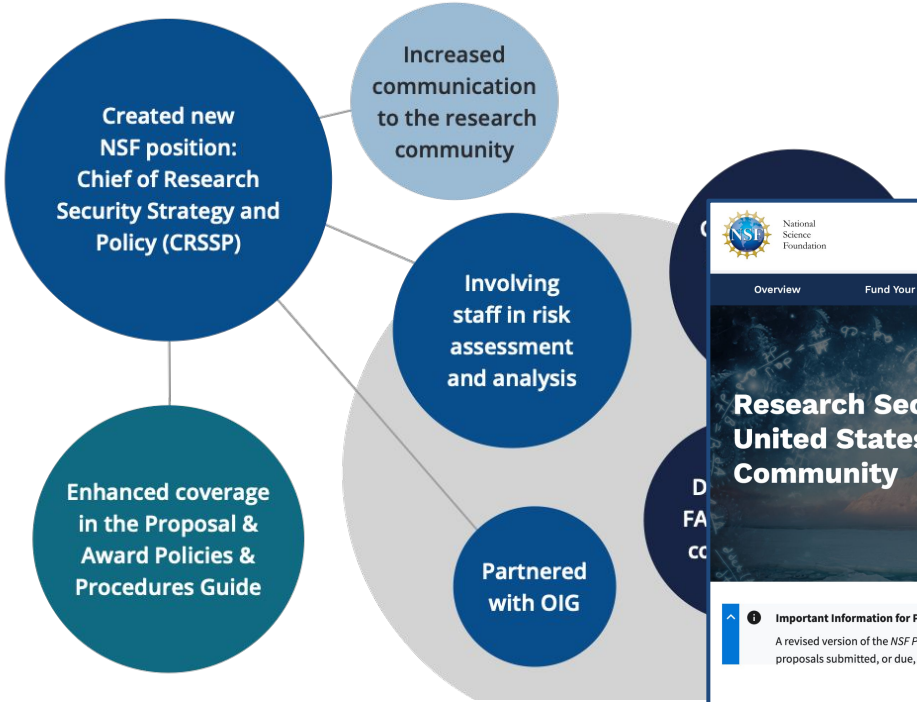
Higher education's challenge with federal cybersecurity: Universities are more like cities than defense contractors.

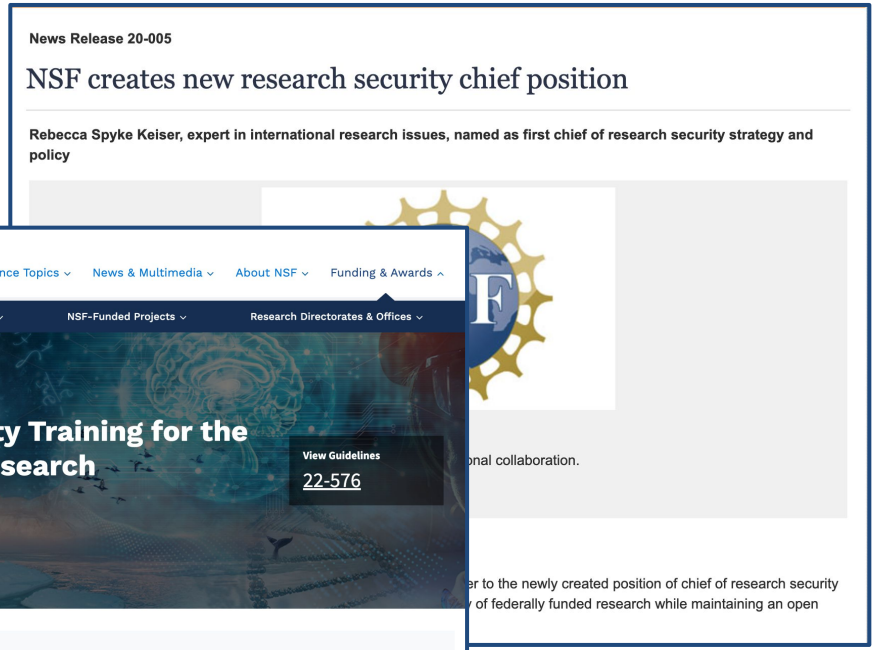
Theater performances, dorms, libraries, DoD research, NIH research, NSF research, sporting events, etc. - all next door to each other.

My Talk


NSF
Image credit: Pixabay https://www.pexels.com/photo/black-textile-41949/

NSF's Actions in Research Security





News Release 20-005

NSF creates new research security chief position

Rebecca Spyke Keiser, expert in international research issues, named as first chief of research security strategy and policy

...nal collaboration.

...r to the newly created position of chief of research security ...y of federally funded research while maintaining an open

National Science Foundation

Science Topics | News & Multimedia | About NSF | Funding & Awards

Overview | Fund Your Research | NSF-Funded Projects | Research Directorates & Offices

Research Security Training for the United States Research Community

View Guidelines 22-576

Important Information for Proposers

A revised version of the *NSF Proposal & Award Policies & Procedures Guide* (PAPPG) (NSF 22-1), is effective for proposals submitted, or due, on or after October 4, 2021. Please be advised that, depending on the specified

Print this Page

Synopsis

With the goal of strengthening research security in the U.S., NSF is working in partnership with three other federal research funding agencies to find a balanced approach to research security. This effort includes the development and implementation of training—to recipients of federal research funding—in best practices to optimize research security. This training is an essential step toward mitigating foreign government risks and threats to U.S. government-funded research and may be used to fulfill the research security program requirement in NSPM-33.

Upcoming Due Dates

Full Proposal

2022

May 23 - Deadline Date

Program Guidelines

https://beta.nsf.gov/research-security
https://beta.nsf.gov/funding/opportunities/research-security-training-united-states-research-community
https://www.nsf.gov/news/news_summ.jsp?cntn_id=300086

JASON Report on Facilities Cybersecurity

The National Science Foundation (NSF) operates 18 major research facilities for the benefit of the scientific research community. Typically, these are one-of-a-kind facilities ranging from telescopes and gravitational wave detectors to oceangoing research vessels and networks of distributed sensors. These facilities operate with the purpose of supplying scientific data openly to the broad community of scientific users. At the same time, the data integrity and the continued operation of these unique NSF-funded scientific assets must be assured. NSF commissioned a study by the JASON advisory group to assess and make recommendations regarding cybersecurity at NSF's major facilities so as to sustain their ability to provide high-quality data to the research community while mitigating potential cybersecurity threats. NSF received the JASON report (Executive Summary here) containing 13 findings and 7 recommendations. NSF agrees with all the recommendations in the report; responses by NSF may be found below.

1. **Recommendation:** NSF should maintain its current approach of supporting major facilities to enhance cybersecurity through assessments of risk, and development and implementation of mitigation plans. A prescriptive approach to cybersecurity should be avoided because it would be a poor fit to the diversity of facilities, would inefficiently use resources, and would not evolve quickly enough to keep up with changing threats.

   NSF response: NSF intends to maintain its current philosophy of performing oversight of awardee plans that are tailored to the unique natures of the individual major facilities. Through its review processes, NSF will ensure that these plans are consistent with best practices for cybersecurity that are in common between major research facilities and other types of infrastructure.

https://www.nsf.gov/news/special_reports/jasonreportcybersecurity/index.jsp
See also: https://blog.trustedci.org/2022/03/trusted-ci-applauds-jason-report-on.html

A Growing Set of NSF Cybersecurity Resources….

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

CILogon

ResearchSOC

https://www.trustedci.org/ - https://www.regulatedresearch.org/ - https://www.cilogon.org/ - https://researchsoc.iu.edu/
https://beta.nsf.gov/funding/opportunities/cybersecurity-innovation-cyberinfrastructure-cici

The Trusted CI Framework

Four Pillars. Sixteen Musts. An Architecture for Cybersecurity Programs

Mission Alignment

1. Organizations must tailor their cybersecurity programs to the organization's **mission**.
2. Organizations must identify and account for cybersecurity **stakeholders and obligations**.
3. Organizations must establish and maintain **documentation of information assets**.
4. Organizations must establish and implement a structure for **classifying information assets** as they relate to the organization's mission.

Governance

5. Organizations must **involve leadership** in cybersecurity decision making.
6. Organizations must formalize roles and responsibilities for cybersecurity **risk acceptance**.
7. Organizations must establish a **lead role** with responsibility to advise and provide services to the organization on cybersecurity matters.
8. Organizations must ensure the cybersecurity program **extends to all entities** with access to, control over, or authority over information assets.
9. Organizations must develop, adopt, explain, follow, enforce, and revise cybersecurity **policy**.
10. Organizations must **evaluate and refine** their cybersecurity programs.

Resources

11. Organizations must devote **adequate resources** to address unacceptable cybersecurity risk.
12. Organizations must establish and maintain a cybersecurity **budget**.
13. Organizations must allocate **personnel** resources to cybersecurity.
14. Organizations must identify **external cybersecurity resources** to support the cybersecurity programs.

Controls

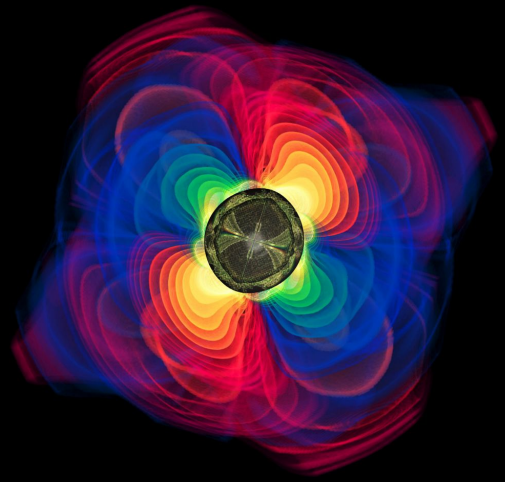
15. Organizations must adopt and use a **baseline control set**.
16. Organizations must select and deploy **additional and alternate controls** as warranted.

Visit www.trustedci.org/framework to learn more.

National Science Foundation
WHERE DISCOVERIES BEGIN

RESEARCH INFRASTRUCTURE GUIDE

NSF guidance for full life-cycle oversight of Major Facilities and Mid-Scale Projects



NSF Large Facilities Office
Office of Budget, Finance and Award Management

NSF 21-107
December 2021

Credit: Scientific contact by Ed Seidel (eseidel@aci.mpg.de); simulations by Max Planck Institute for Gravitational Physics (Albert-Einstein-AEI); visualization by Werner Benger, Zuse Institute, Berlin (ZIB) and AEI. The computations were performed on NCSA's Ir.

https://www.trustedci.org/framework/core - https://www.nsf.gov/pubs/2021/nsf21107/nsf21107.pdf

Thank yous

Materials from Scott Shackelford and Michael Corn.

Trusted CI is supported by the National Science Foundation under Grants 1234408, 1547272, and 1920430.

trustedci.org

ResearchSOC is supported by the National Science Foundation under Grant 1840034.

researchsoc.iu.edu

INDIANA UNIVERSITY