Insider Threat Awareness

Federal Select Agent Program
Responsible Official Workshop
United States Department of Agriculture
July 23, 2019

William "Will" So, Ph.D.
Policy & Program Specialist
FBI Headquarters
Weapons of Mass Destruction Directorate
Biological Countermeasures Unit

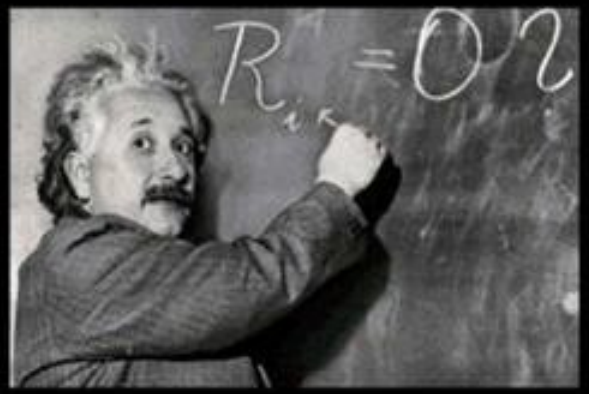
What is Scientific Research?

what my mom thinks I do

what my friends think I do

what society thinks I do

what my boss thinks I do



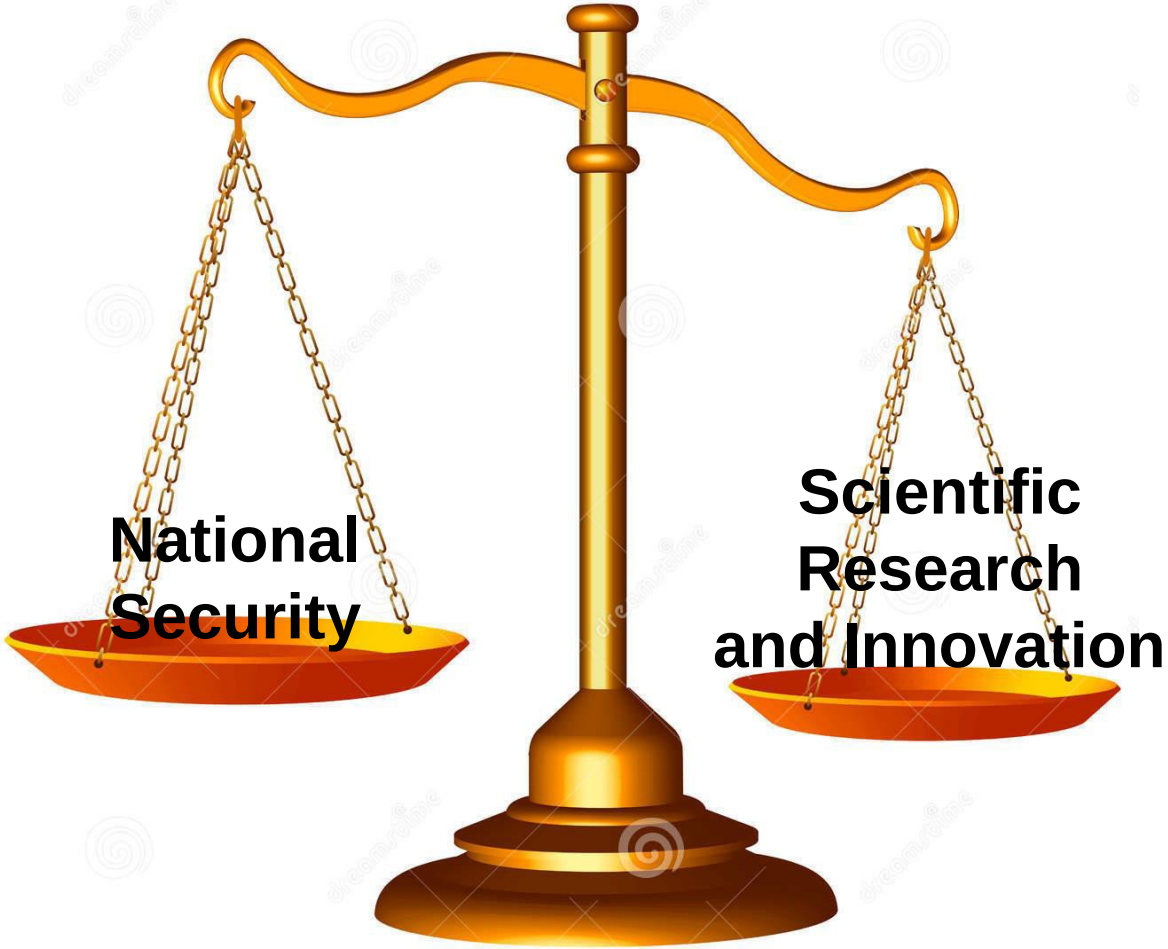
what I think I do

What I really do

What is National Security?

What do they have in common?

It Should Not be Rocket Science!

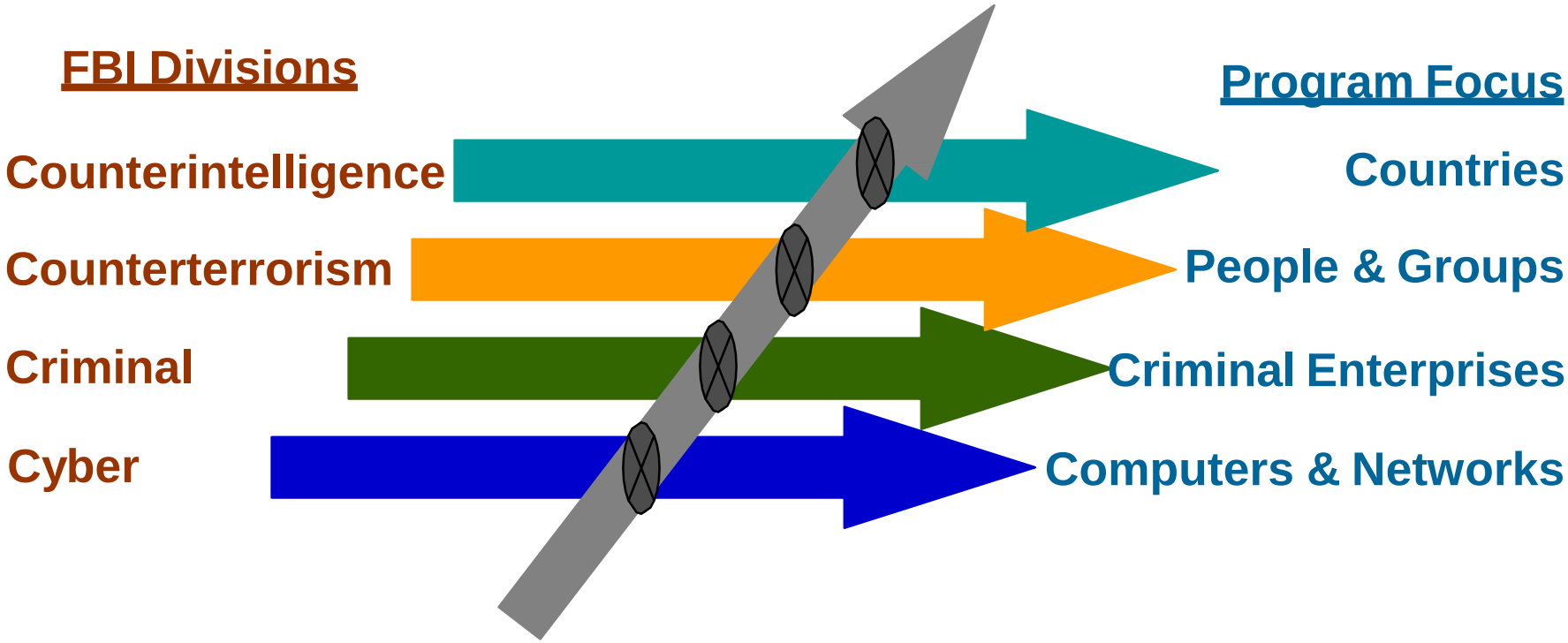


Weapons of Mass Destruction Directorate

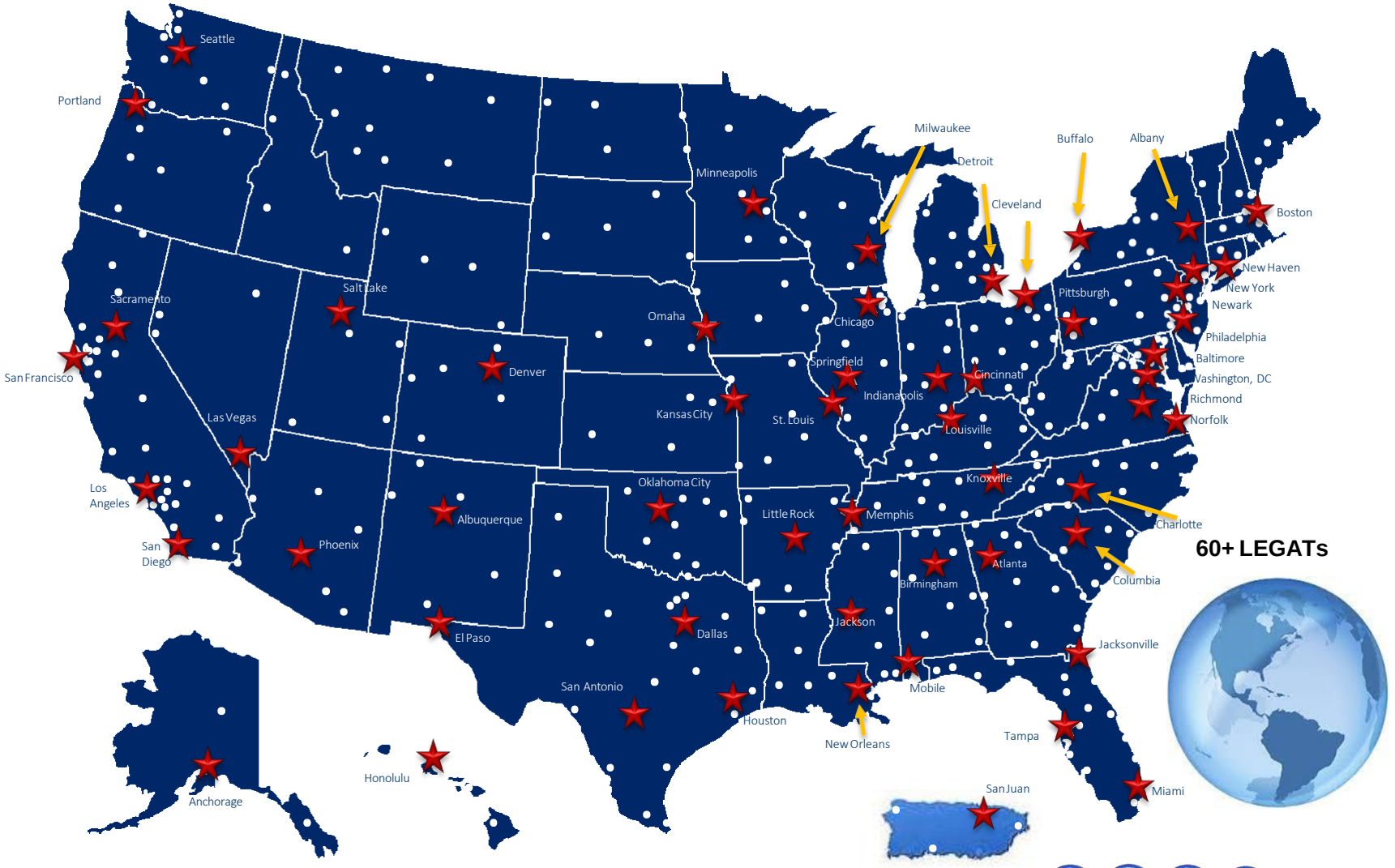
Integrated Sections of the WMDD

July 2006

1. **Countermeasures Operations**
2. **Investigative and Operations**
3. **Intelligence Analysis**



FBI FIELD OFFICES



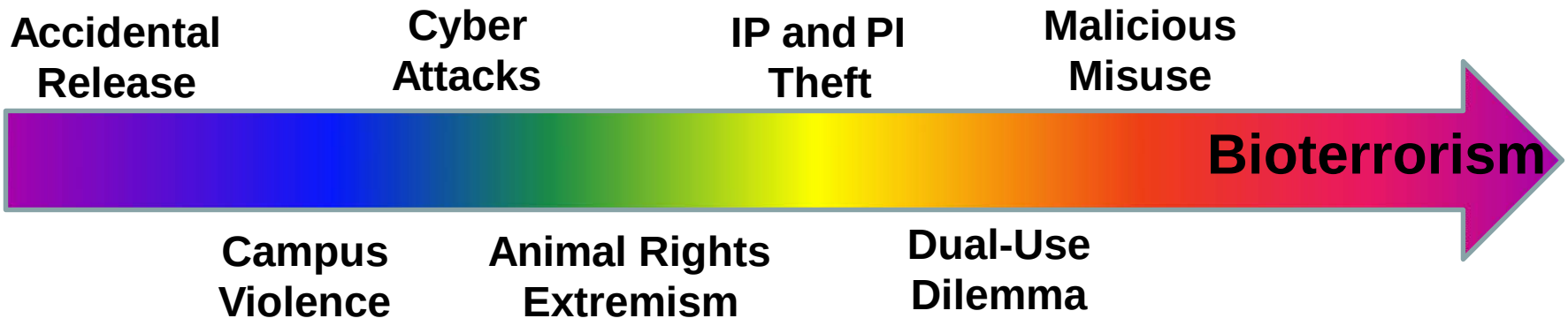
WMD Coordinator and Their Role

- At least one WMD Coordinator in all of the FBI's 56 Field Offices
- Contacted by state and local Emergency Responders when confronted by a WMD threat or incident
- Act as a conduit to FBIHQ and the Federal Government for technical information, advice, and assistance
- Emphasis on pre-event planning and prevention
- Liaison with Federal regional counterparts, state, county and local response agencies, private industry and academia

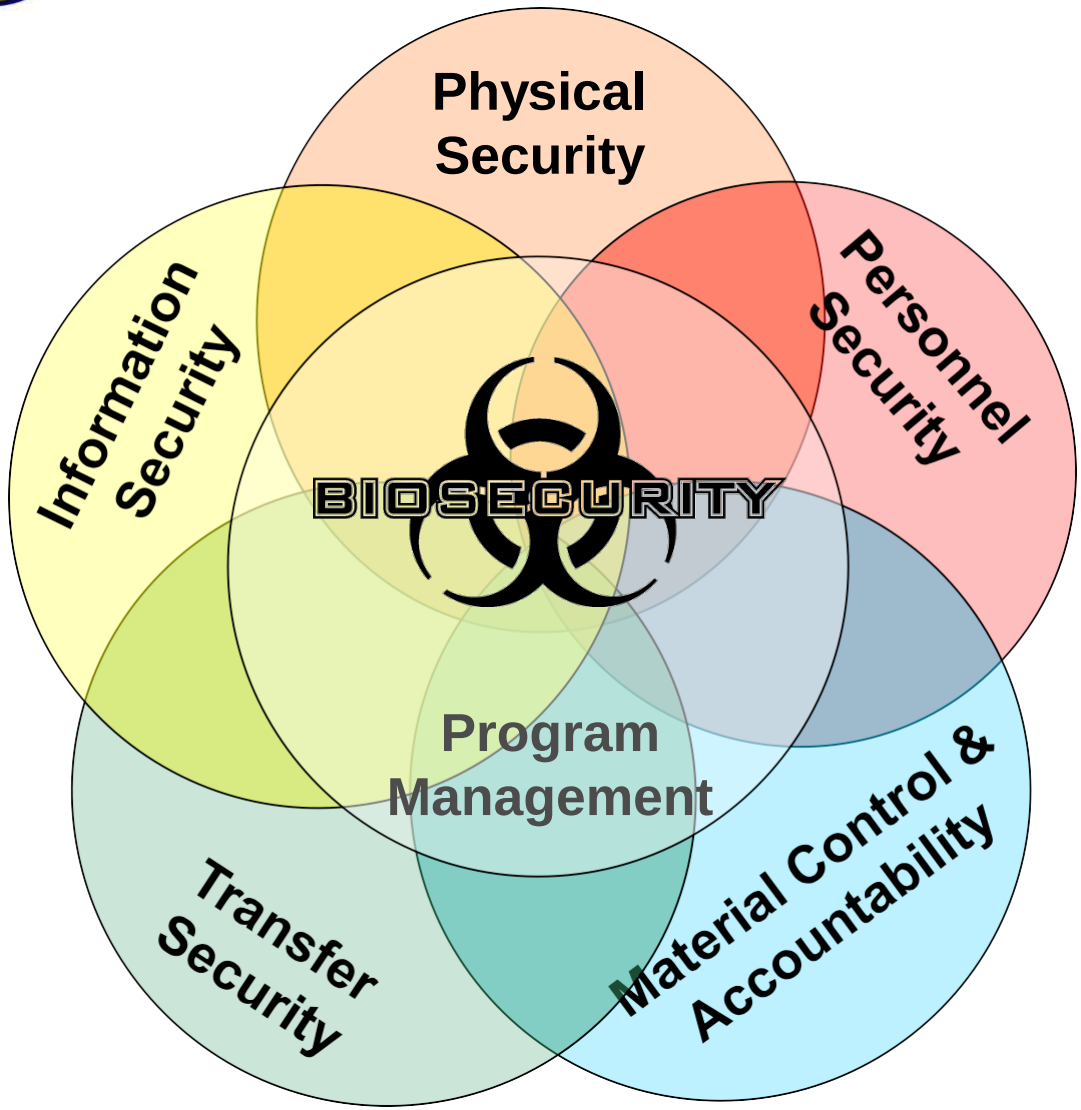
FBI WMD Biological Countermeasures Unit's Objectives

- ✓ Build national and international bioterrorism threat detection, prevention strategies, identification of over-the-horizon challenges, and reporting capabilities
- ✓ Improve bioterrorism and risk assessment and investigative capabilities
- ✓ Enhance scientific, industry, and academic outreach and awareness

Biosecurity Spectrum



Biosecurity Program Components



- Places
- People
- Things
- Information

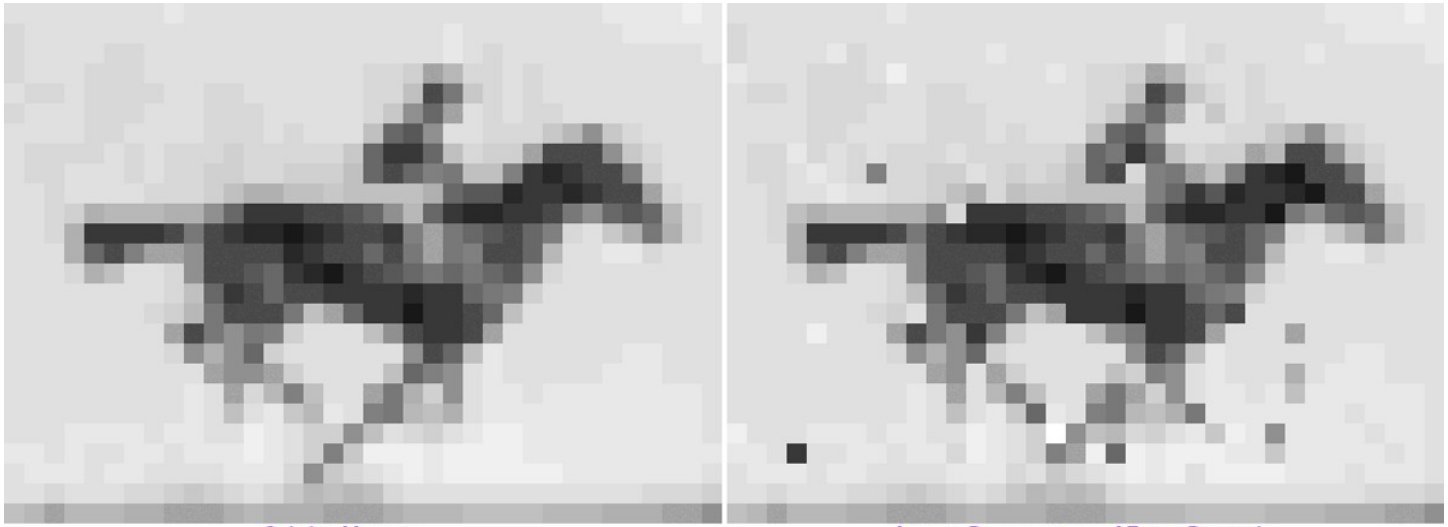
How is Biosecurity Viewed by Others?

Blessing or Curse

“May you live in interesting times”

Expression attributed to a collection of short stories from the 17th Century.

寧為太平犬莫做亂離人

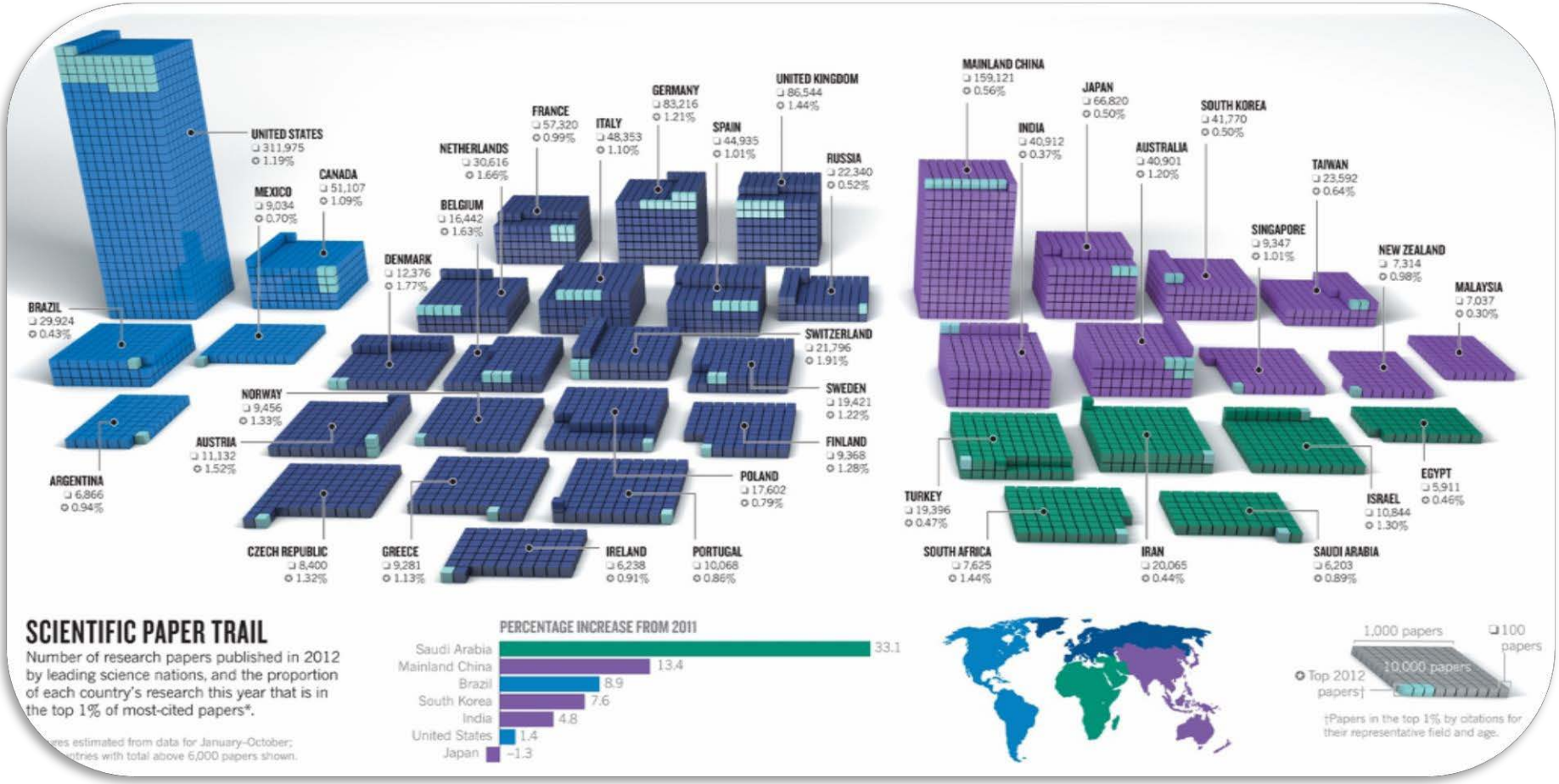


Original Image

Image Reconstructed From Bacteria

https://www.zmescience.com/science/news-science/gif-bacteria-crispr-4432/

Lead in Scientific Research…still?



https://infoproc.blogspot.com/2013/01/scientific-publications-by-country.html

Why is Gene Editing Research Important?

Graphic courtesy of Dr. Kenneth Oye, MIT

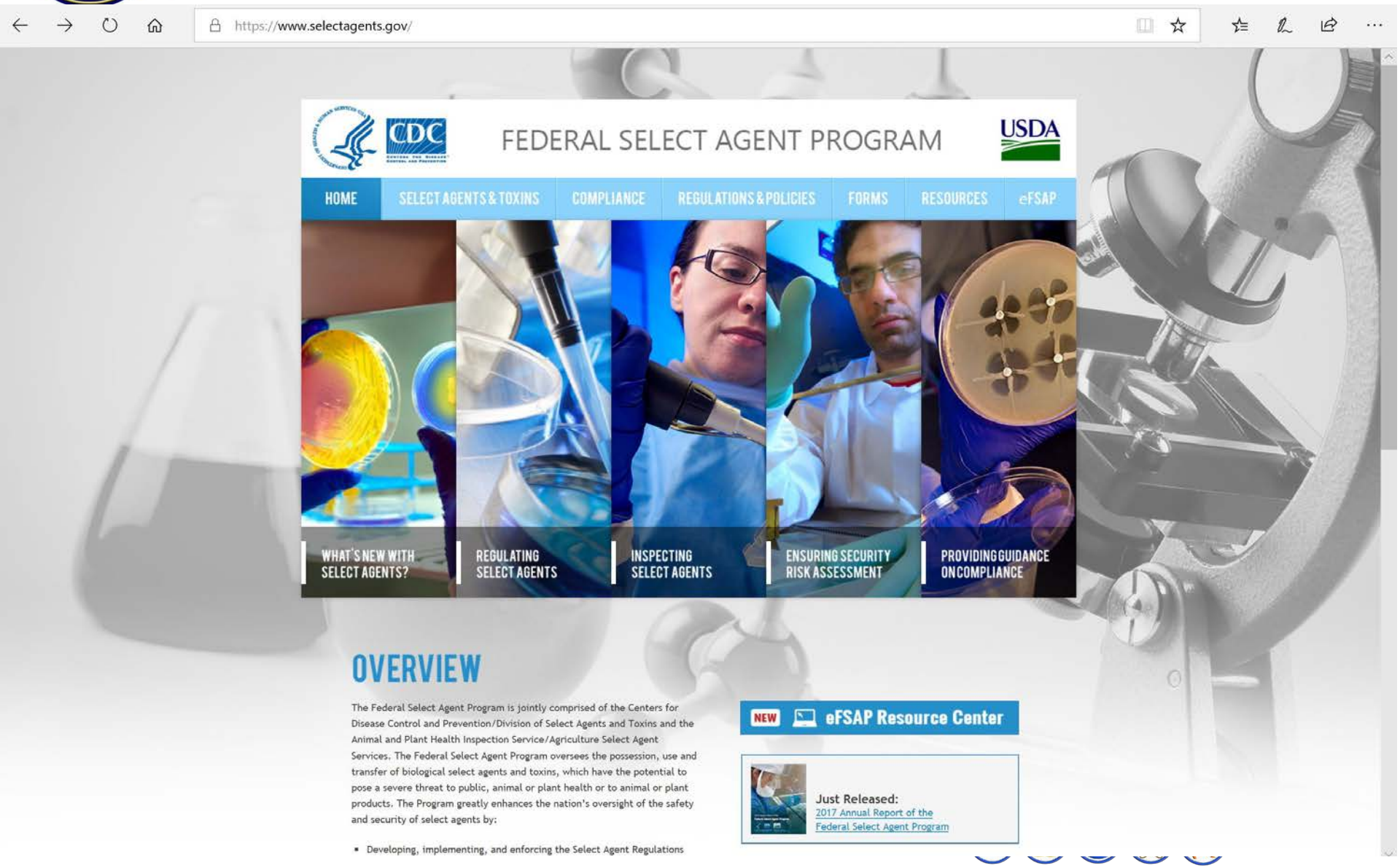
Σ

25% GDP

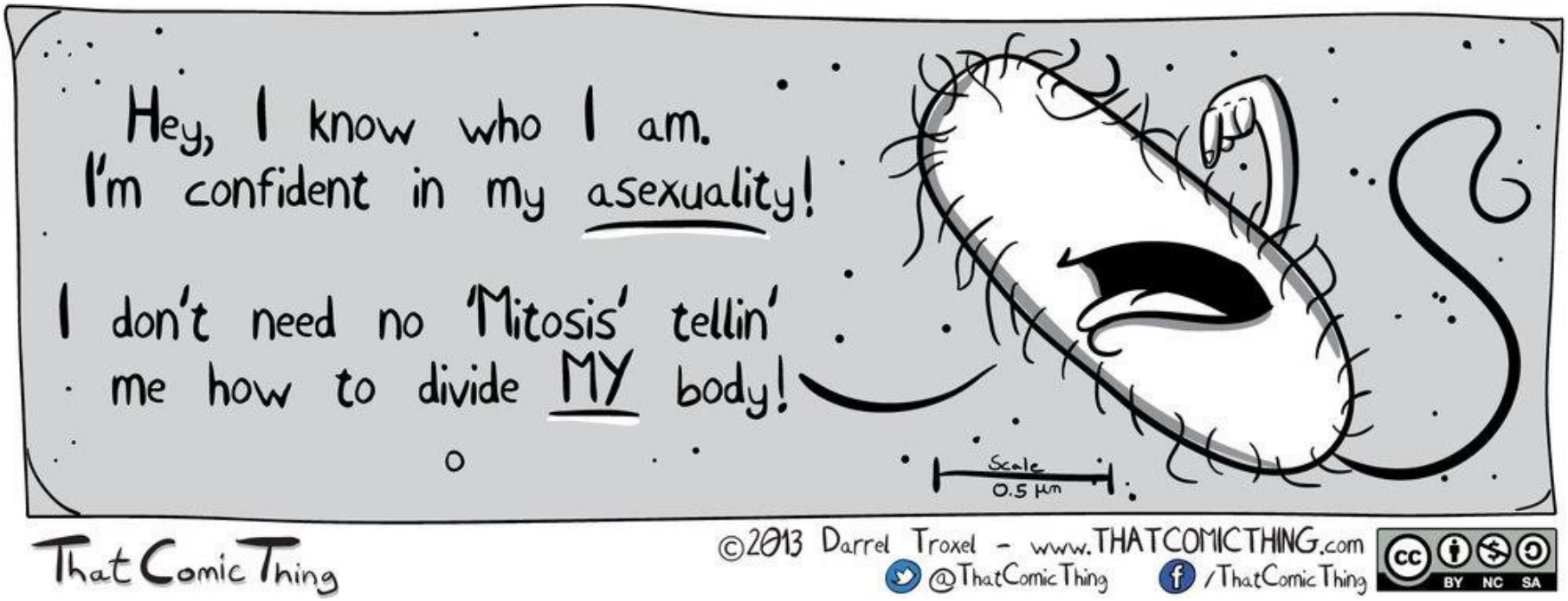
$4 Trillion

BIOLOGICAL MATERIAL SECURITY - CHALLENGING

Guidance from the Federal Select Agent Program



Inventory - Challenges



https://thatcomicthing.com/tag/binary-fission/

Will Technology be the Solution?

U.S. Army Testing RFID for Medical Biodefense Management

The military's medical research lab has been applying RFID labels to biological samples for vaccine, drug and infectious disease management research, to ensure that the samples can be identified in freezers without being removed from cold storage.

By Claire Swedberg

Tags: Defense, Health Care, Inventory / Warehouse Management, Labeling, Pharmaceuticals

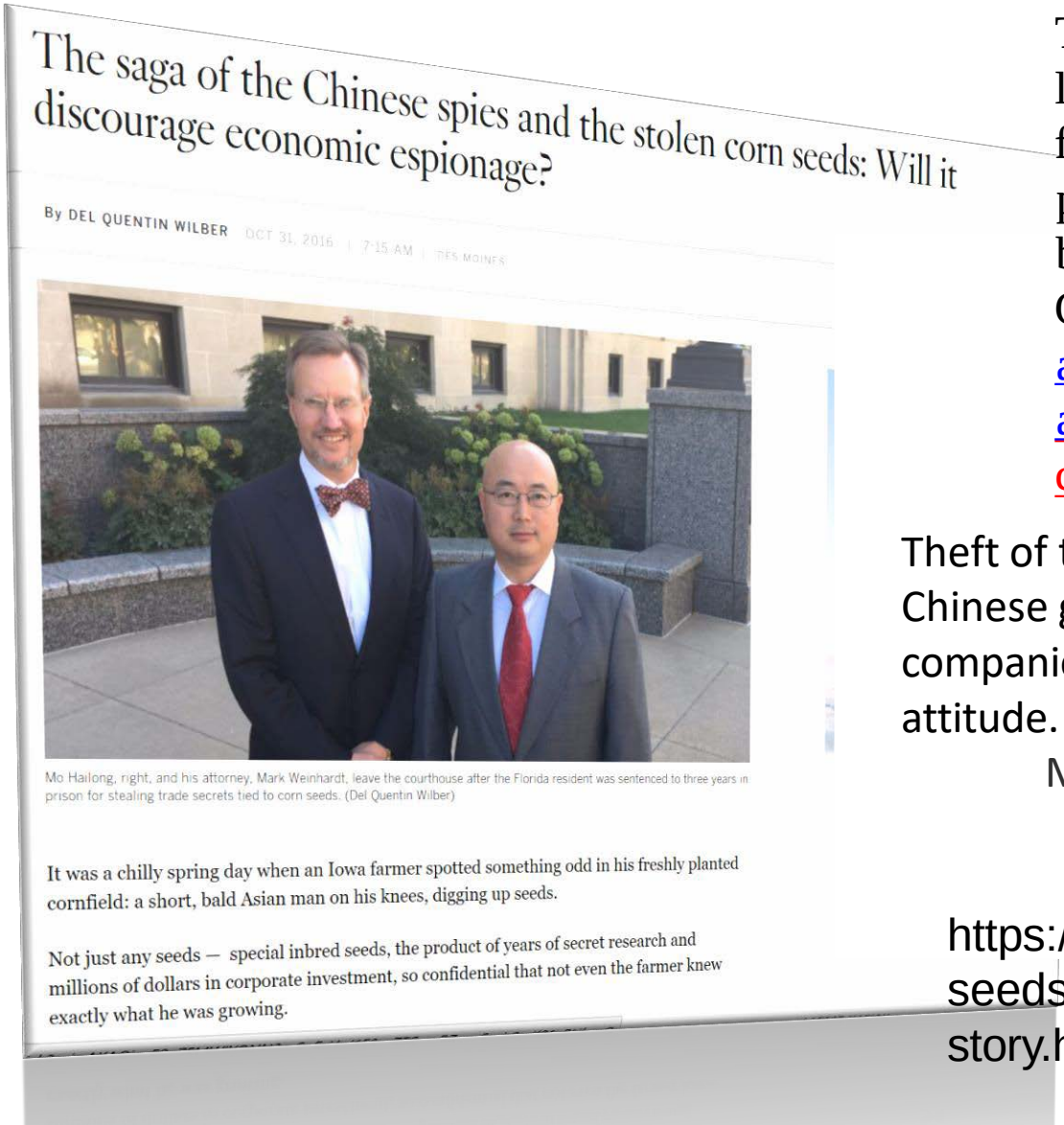
PDF | Email | Print | Definitions | Save Article

May 24, 2019—When some of the most sensitive biological samples are stored in laboratories, even removing them from freezers for a minute could increase their temperature. That means the manual process of inventory counting could pose a risk to the samples themselves. Therefore, the U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID) has spent the last two years testing an RFID–based solution that may enable it to count its highly sensitive samples without removing them from freezers. The agency is presently testing UHF RFID tags and readers at its lab in Fort Detrick, Md.

USAMRIID (pronounced "you–SAM–rid") conducts research on developing medical countermeasures against biological threats aimed at U.S. troops. It employs military and civilian scientists and collaborates with the Centers for Disease Control and Prevention, the World Health Organization, and multiple biomedical and academic institutes around

https://www.vox.com/future-perfect/2019/3/20/18260669/deadly-pathogens-escape-lab-smallpox-bird-flu

Material Security – Field Studies



The saga of the Chinese spies and the stolen corn seeds: Will it discourage economic espionage?

By DEL QUENTIN WILBER OCT. 31, 2016 | 7:15 AM | DES MOINES

Mo Hailong, right, and his attorney, Mark Weinhardt, leave the courthouse after the Florida resident was sentenced to three years in prison for stealing trade secrets tied to corn seeds. (Del Quentin Wilber)

It was a chilly spring day when an Iowa farmer spotted something odd in his freshly planted cornfield: a short, bald Asian man on his knees, digging up seeds.

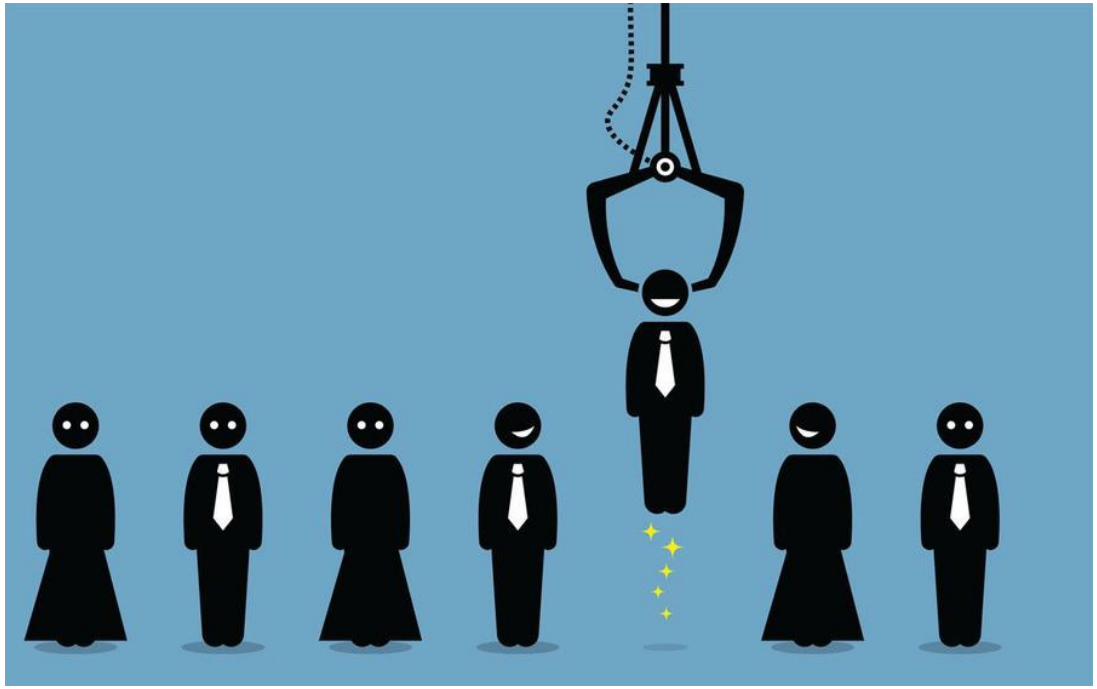
Not just any seeds — special inbred seeds, the product of years of secret research and millions of dollars in corporate investment, so confidential that not even the farmer knew exactly what he was growing.

That curious encounter eventually led to an exhaustive five-year federal investigation and prosecution into one of the most brazen examples of Chinese economic espionage against the U.S., a crime that annually costs American companies at least $150 billion.

Theft of trade secrets is not only promoted by Chinese government policies and state-backed companies, but it also reflects their societal attitude.

MELANIE REID, PROFESSOR AT LINCOLN MEMORIAL UNIVERSITY DUNCAN SCHOOL OF LAW

https://www.latimes.com/nation/la-na-seeds-economic-espionage-20161031-story.html



PERSONNEL SUITABILITY AND RELIABILITY

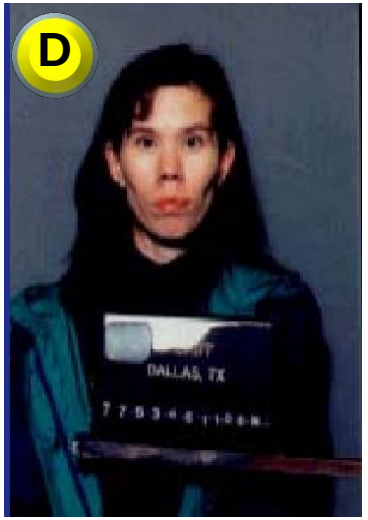
Criteria for a Scientist?

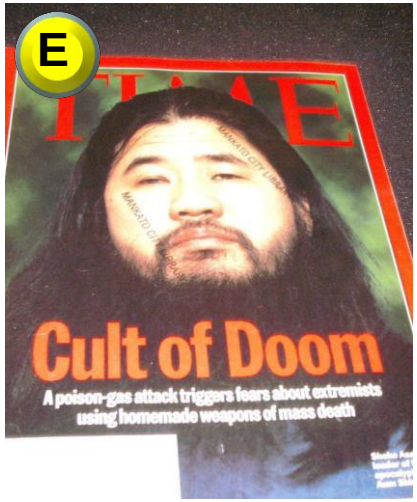
- Accuracy
- Work Ethic
- Publication Record
- Education
- Abilities in the lab
- Technical competency
- Creativity
- Determination
- Perseverance
- Collaboration
- Communication Skills

Criteria for a Babysitter?

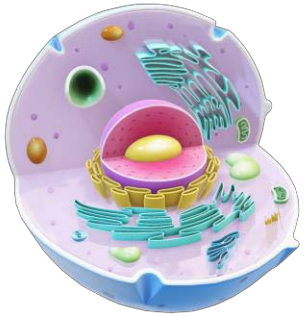
- Reliability
- Trustworthiness
- Compassion
- Honesty
- Responsible
- Stability
- Non-violent
- Kind
- Follow Rules
- Good Judgment
- Driving Record

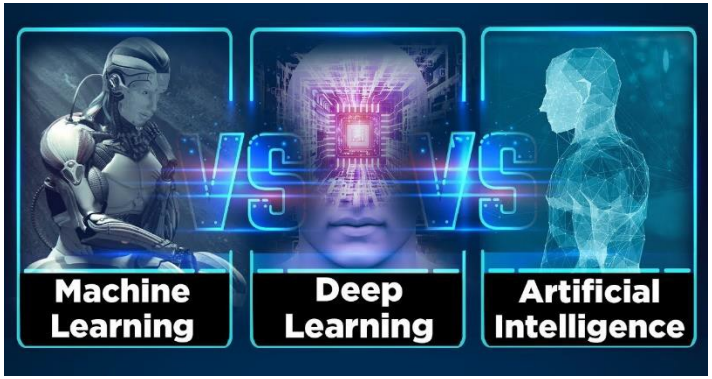
Insider Threats





Scope of Cyberbiosecurity





Biology **Physical** **Cyber**

CYBERBIOSECURITY

Cyberbiosecurity

- The convergence among cyber security, cyber physical security, and biological security
- Not simply an awareness raising and improve collaboration, but possible new discipline

https://www.frontiersin.org/research-topics/8353/mapping-the-cyberbiosecurity-enterprise

Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy

Randall S. Murch[1]*, William K. So[2], Wallace G. Buchholz[3], Sanjay Raman[1] and Jean Peccoud[4]

[1] Virginia Tech – National Capital Region, Virginia Polytechnic Institute and State University, Arlington, VA, United States, [2] Weapons of Mass Destruction Directorate, Federal Bureau of Investigation, Washington, DC, United States, [3] Biological Process Development Facility, University of Nebraska, Lincoln, NE, United States, [4] Department of Chemical and Biological

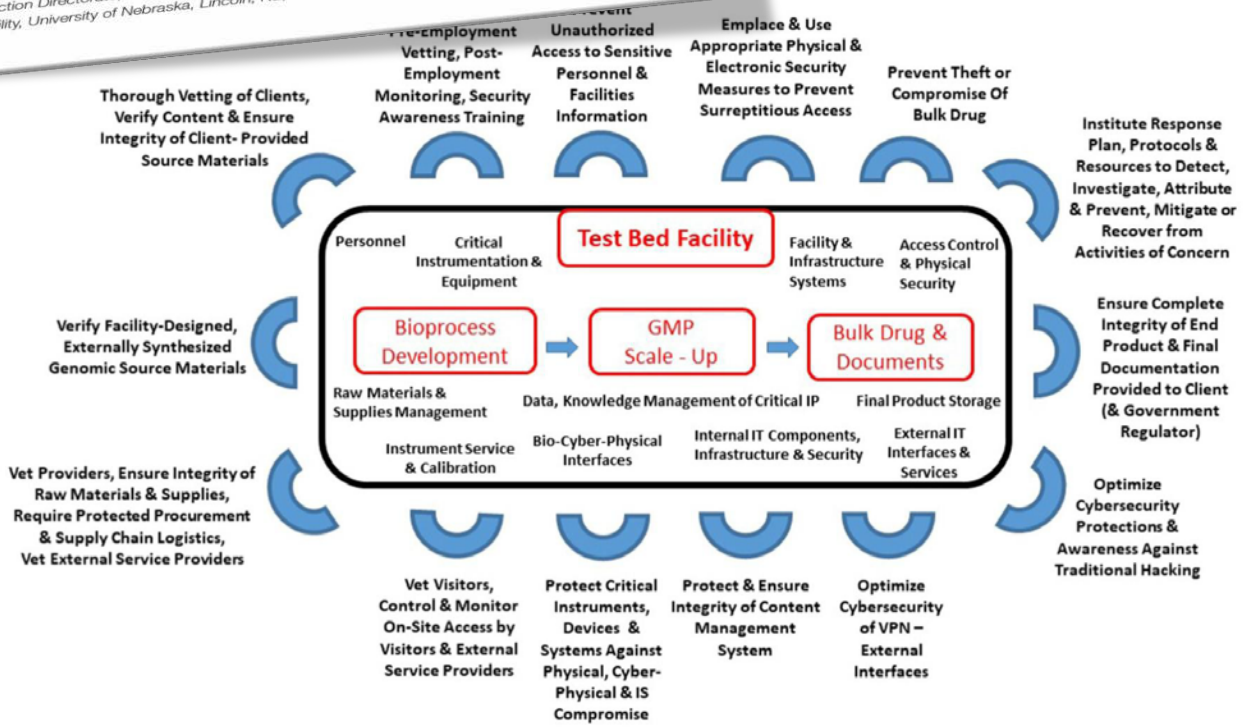


FIGURE 1 | A systems view of protecting a biomanufacturing facility. For each defensive set identified, multiple threats and impacts were identified and potentially more than one pathway or technique could be used by an adversary to achieve their objectives. GMP, Good Manufacturing Practice; IT, Information Technology; IS, Information Systems; VPN, Virtual Private Network; IP, Intellectual Property.

Iranian hackers attacked college professors…

"The hackers did their homework," the cyber agent said. They conducted online reconnaissance of professors to determine the individuals' research interests and the academic articles they had published.

- Targeted 100K+ US professors' email accounts at 144 universities – spearphising
- Successfully compromised ~ 8K accounts, > 3700 U.S. professors
- 176 foreign universities and ~ 50 U.S. and international companies
- Estimated cost of $3.4B
- Mabna Institute, Iran-based company directed by Iranian Intelligence

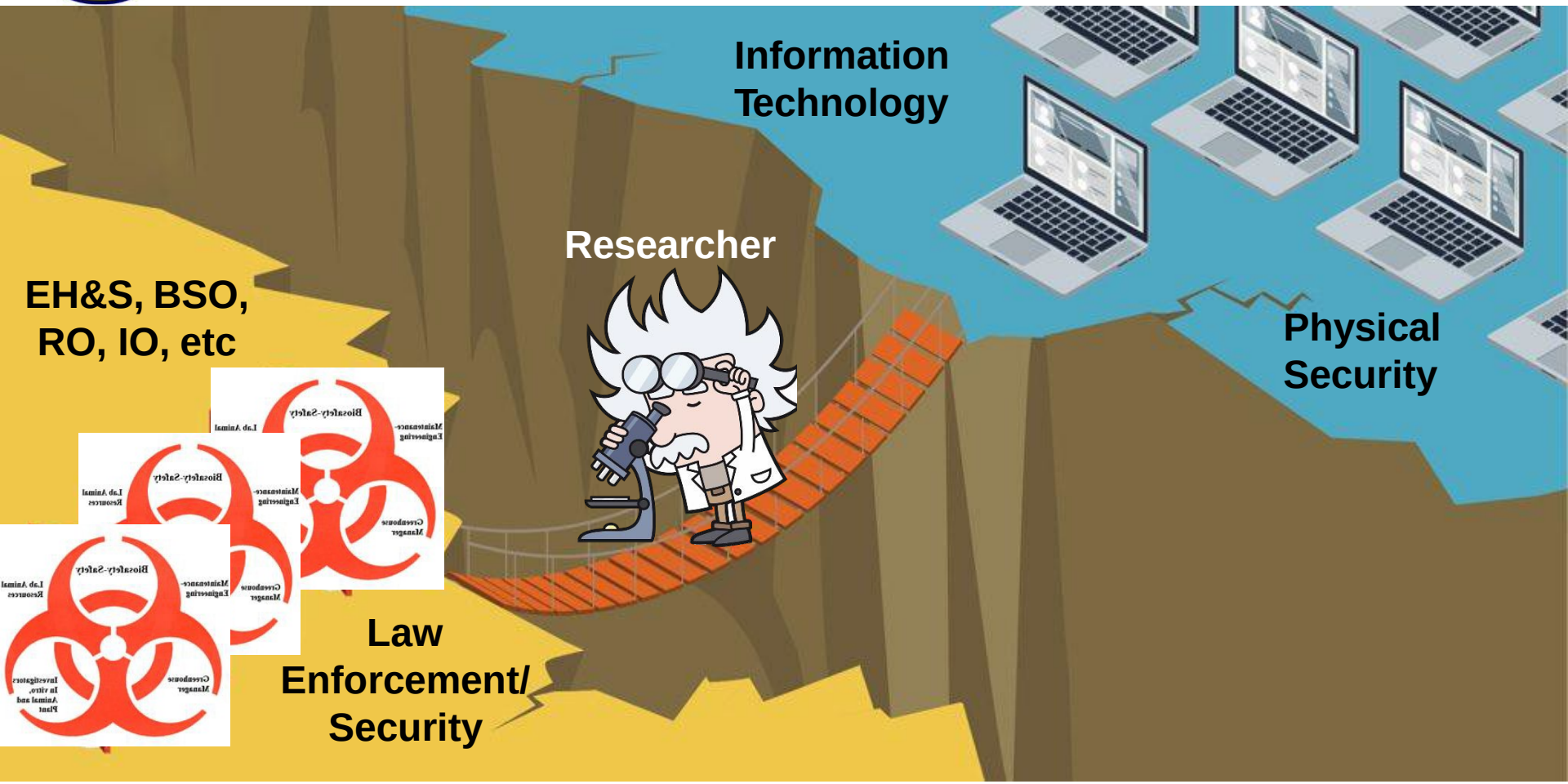
The Iranians targeted data across all fields of research and academic disciplines, including science and technology, engineering, social sciences, medical, and other professional fields.

https://www.cnbc.com/2018/03/23/us-indicts-iranian-nationals-in-iran-government-backed-scheme-on-us-universities.html

https://www.fbi.gov/news/stories/nine-iranians-charged-in-hacking-scheme-032318

March 23, 2018

Where Do They Interface - Currently

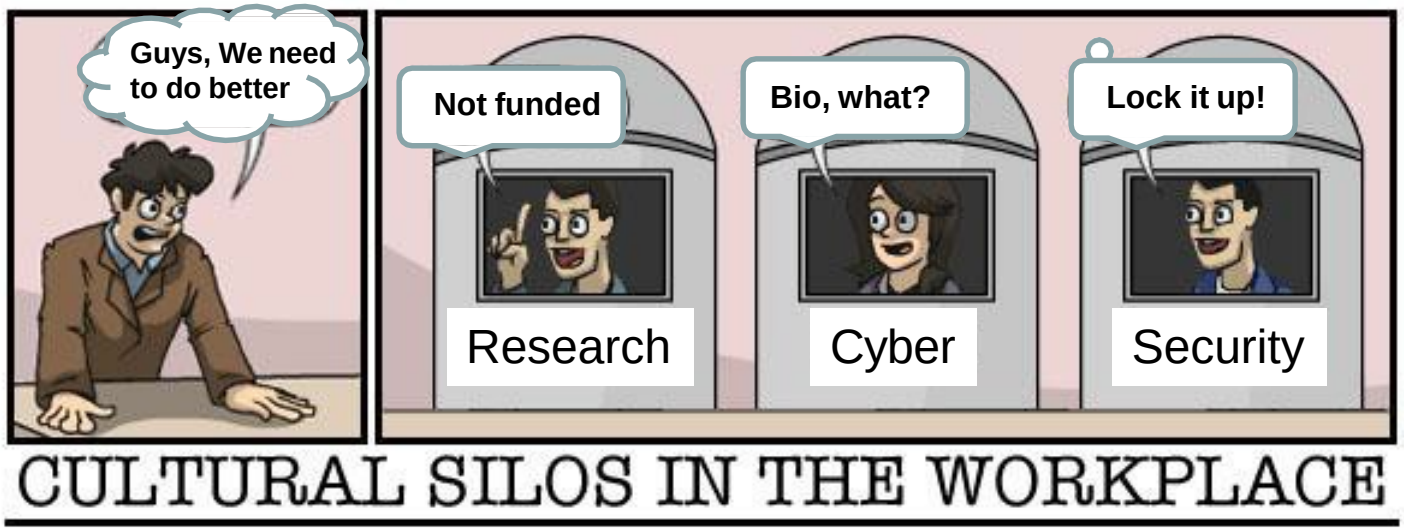


Realities of Cyber Security

Does security stand alone?

Does your company have a security executive in the c-suite, and if so, who do they report to? The question goes beyond upper-echelon office politics and gets to the heart of who does what in a company, and how they collaborate. For instance, in 75 percent of organizations surveyed in the 2018 IDG Security Priorities study, security and IT teams are part of the same department, with **25 percent having a standalone security department**. But if a company has a dedicated CSO or CISO, they're more likely to have security siloed into a separate department—in such organizations, that happens 40 percent of the time.

https://www.csoonline.com/article/3153707/security/top-cybersecurity-facts-figures-and-statistics.html



The More We Are Connected…

And so are IoT systems

Internet-connected industrial control systems represented the first wave of the internet of things; today, there are millions of IoT devices out there, representing a tempting attack surface that you need to protect. A 2018 report from Trustwave produced some dispiriting numbers when it comes to IoT security:

- 64 percent of surveyed organizations have deployed IoT devices, and another 20 percent plan to do so within the next year
- But only 28 percent of those organizations consider their IoT security strategy to be "very important," and more than a third think it's only somewhat important, or not important at all

Take those two facts into consideration, and is it any surprise that **61 percent of those surveyed have already experienced an IoT security incident**?

Current Cyber Issues

Email is still the problem

Are you tired of sending out nagging notes to company staffers insisting that they not just click on any old email attachments? Well, we're afraid you're going to have to keep at it, because according to Verizon's 2018 Breach Investigations report, **92 percent of malware is still delivered by email**.

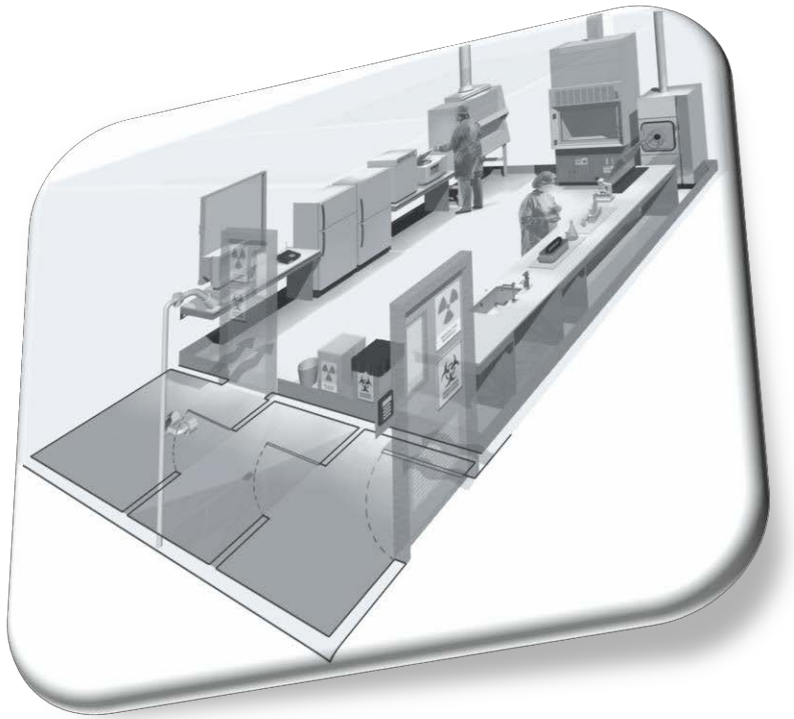
One of the most common methods of email malware infection is through phishing attacks, which are becoming increasingly targeted. And security pros are taking notice. Out of the 1,300 IT security decision makers surveyed for CyberArk Global Advanced Threat Landscape Report 2018, **56 percent said that targeted phishing attacks were the top security threat they faced**.

https://www.csoonline.com/article/3153707/security/top-cybersecurity-facts-figures-and-statistics.html

Has there be cyber intrusions – other than…

Unfortunately, it has happened

1. Federal Facility
2. Non-Federal Facility



The Value of the Information

The company's data was put to use in a study published this month that found 124 genetic variants associated with a person's willingness to engage in risky behaviors like drinking, smoking, speeding and having multiple sexual partners.

In another study, **23andMe partnered with drug company Pfizer to identify for the first time a collection of the genetic markers for depression.**

23andMe is well known for its DNA kits that promise to shed light on a person's ancestral history and potential health risks.

But the Silicon Valley company has **quietly evolved into a driving force for medical research, experts say.**

By harnessing its massive trove of genetic data, 23andMe has notched more than **110 peer-reviewed publications and launched its own therapeutics lab.** Outside researchers and pharmaceutical companies have lined up to collaborate with the firm, drawn by its ocean-sized pool of data derived from the more than 4 million customers who have agreed to let their DNA test results be used in research.

https://www.nbcnews.com/health/health-news/dna-test-company-23andme-now-fueling-medical-research-n958651

(U) Medical Record Hacks

- (U) Since 2010, 274 different companies with IT incidents, affecting more than 128 million individuals.

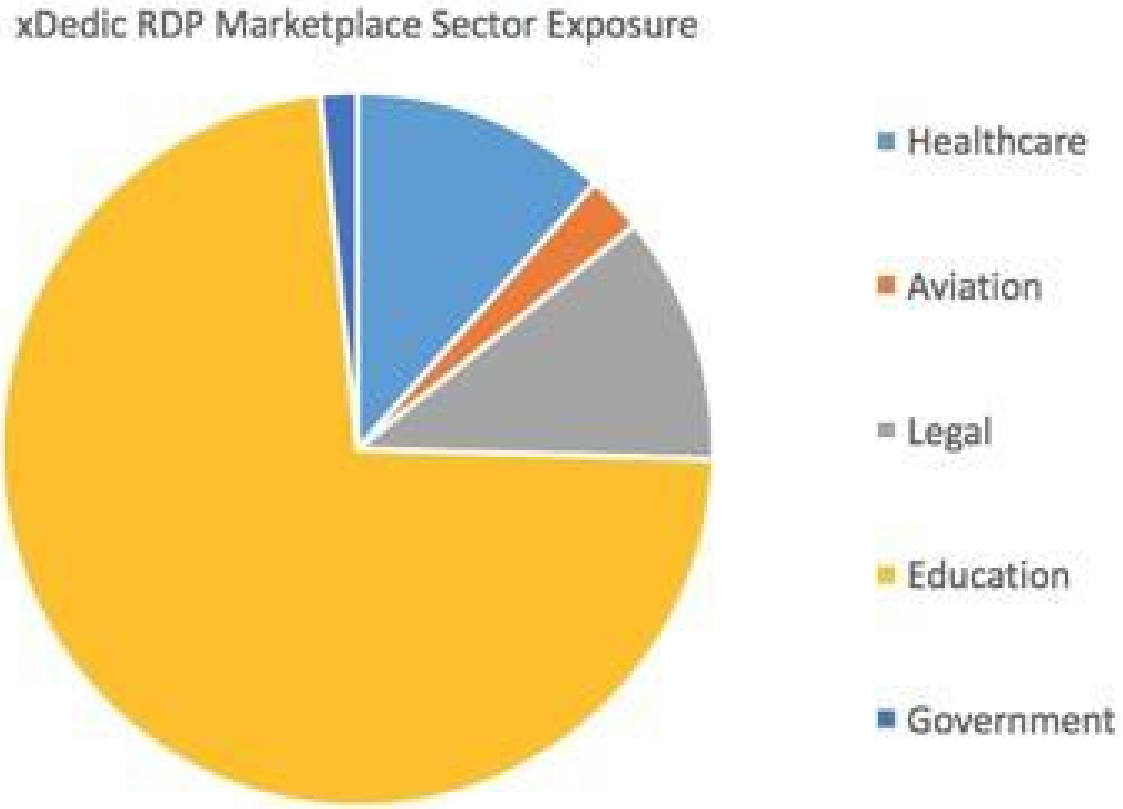
Hacks:

- (U) Premera Blue Cross Blue Shield, 11 million patient records (Mar. 2015)*
- (U) Quest Diagnostics, 34,000 individuals. (Nov 2016)*
- (U) UCLA Health System, 4.5 million patient records (Jul. 2015)*
- (U) Excellus Health Plan Inc, 10.5 million individuals.(Sept 2015)*
- (U) Community Health Systems Inc, 4.5 million patient records (Aug. 2014)
- (U) Anthem Blue Cross Blue Shield, 80 million patient records (Jan. 2015)

(U//FOUO) What are the weaknesses in the healthcare information networks?

- Phishing emails are a common vector and 90+% start with a phishing email.
- File Transfer Protocol (FTP) servers
- Remote Desktop Protocol (RDP) is also a common vulnerability exploited by hackers.
- RDP is a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection.
- When you call tech support and they take over your mouse… that's RDP.

(U) What's the market for RDP credentials?



Excerpt from Flashpoint Intel report: "Flashpoint analysts gained access via an external link to one previously-exposed xDedic dataset, which contained information belonging to over 85,000 servers.

What is xDedic?

- A Russian language criminal forum
  - Founded in 2014

- In 2016, the Kaspersky Lab was found to be a major hub of the criminal activities for the sale of compromised servers
  - Kapersky Lab – a multinational cybersecurity and antivirus provider headquartered in Moscow, Russia
  - Moved to the Tor Darkweb Network
  - Areas of focus: online gambling, ecommerce, banks and payment processors, online dating, advertising networks, ISP services, email service providers, web browser and instant messenger services. Various crimeware products were for sale

https://en.wikipedia.org/wiki/XDedic

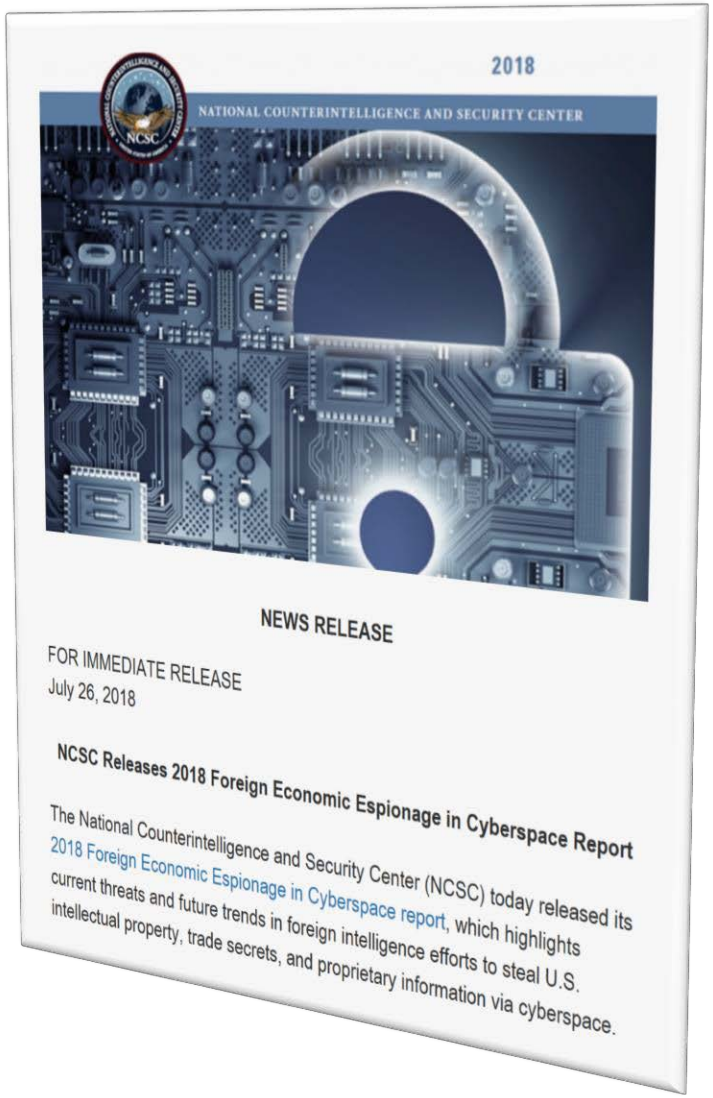
Foreign Strategies – “Trusted” Insiders

China's Strategic Goals

Learning a Hard Lesson - Canada

https://www.the-scientist.com/news-opinion/virologists-escorted-out-of-lab-in-canada-66164

In the 2011 report to Congress on Foreign Spies Stealing U.S. Economic Secrets in Cyberspace, the Office of the National Counterintelligence Executive provided a baseline assessment of the many dangers facing the U.S. research, development, and manufacturing sectors when operating in cyberspace, the pervasive threats posed by foreign intelligence services and other threat actors, and the industries and technologies most likely at risk of espionage. The 2018 report provides additional insight into the most pervasive nation-state threats, and it includes a detailed breakout of the industrial sectors and technologies judged to be of highest interest to threat actors. It also discusses several potentially disruptive threat trends that warrant close attention.


2018

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

NEWS RELEASE

FOR IMMEDIATE RELEASE
July 26, 2018

NCSC Releases 2018 Foreign Economic Espionage in Cyberspace Report

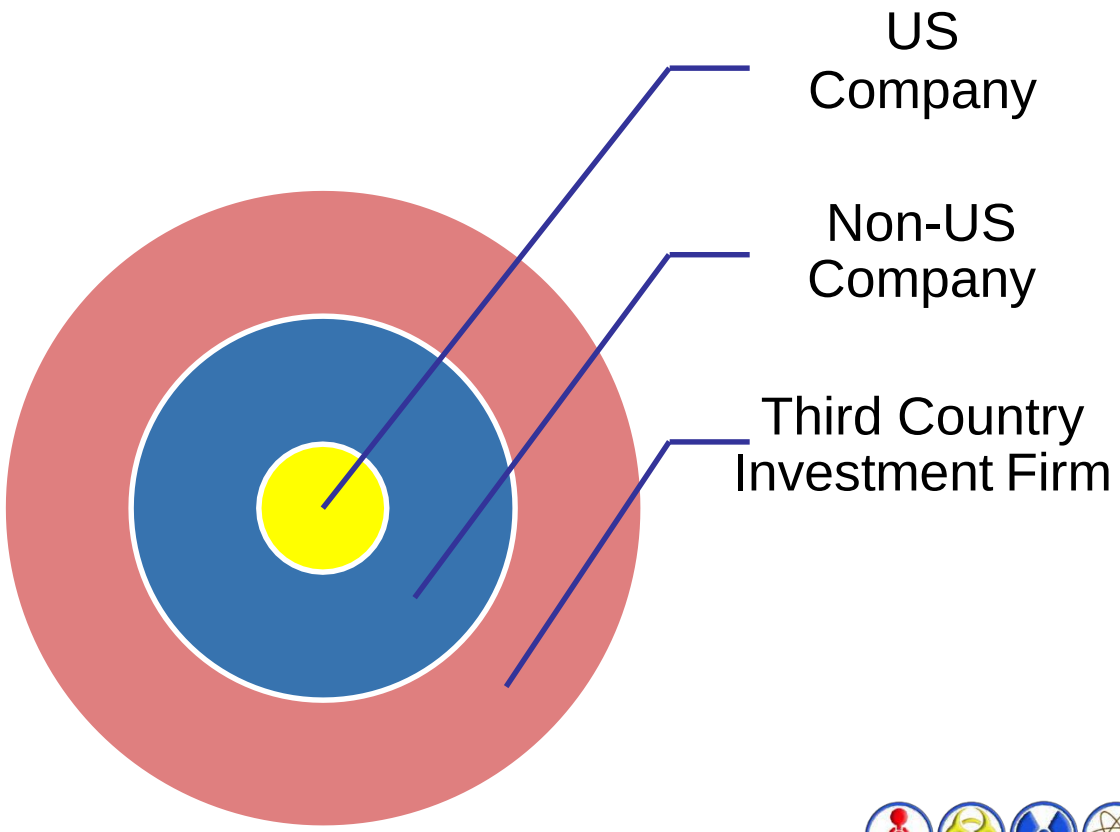
The National Counterintelligence and Security Center (NCSC) today released its 2018 Foreign Economic Espionage in Cyberspace report, which highlights current threats and future trends in foreign intelligence efforts to steal U.S. intellectual property, trade secrets, and proprietary information via cyberspace.

https://www.dni.gov/index.php/ncsc-newsroom/item/1889-2018-foreign-economic-espionage-in-cyberspace

Case Study: Facets of National Security

- Biotechnology and biomedical sector is expected to reach 727.1B USD by 2025; Annual Growth Rate of 7.4%
- Key drivers in regenerative medicine and genetics in diagnosis

(https://www.grandviewresearch.com/press-release/global-biotechnology-market)



THANK YOU

William "Will" So
Policy & Program Specialist, Ph.D.
FBI Headquarters
Weapons of Mass Destruction Directorate
Biological Countermeasures Unit
klwso@fbi.gov