DEPARTMENT OF JUSTICE

Insider Threat Trends

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Updated: 18 Mar 2021

Objectives

1. Discuss current trends in Espionage
2. Discuss current trends in Unauthorized Disclosure
3. Discuss current trends in Workplace Violence
4. Discuss current trends in Domestic Violent Extremism

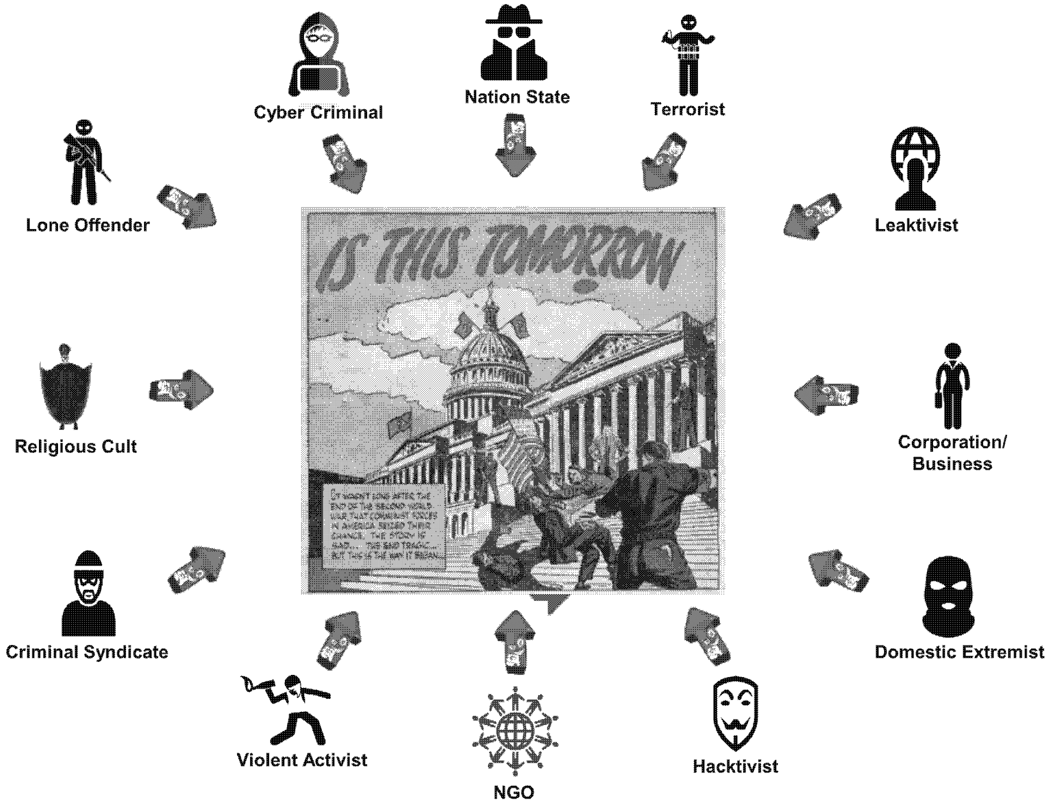
Key Assumptions

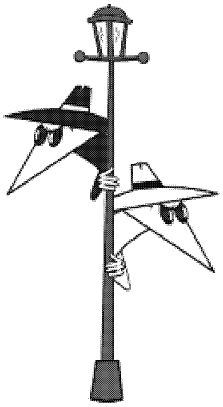
1. Population of US Federal Government/US Military personnel mirror US population

2. Major insider threat event is a rare occurrence – based on low number of reported incidents over the years

3. Risk of a major insider threat event is growing – based on larger number of threat actors, and increased opportunity and vulnerabilities compared to past years

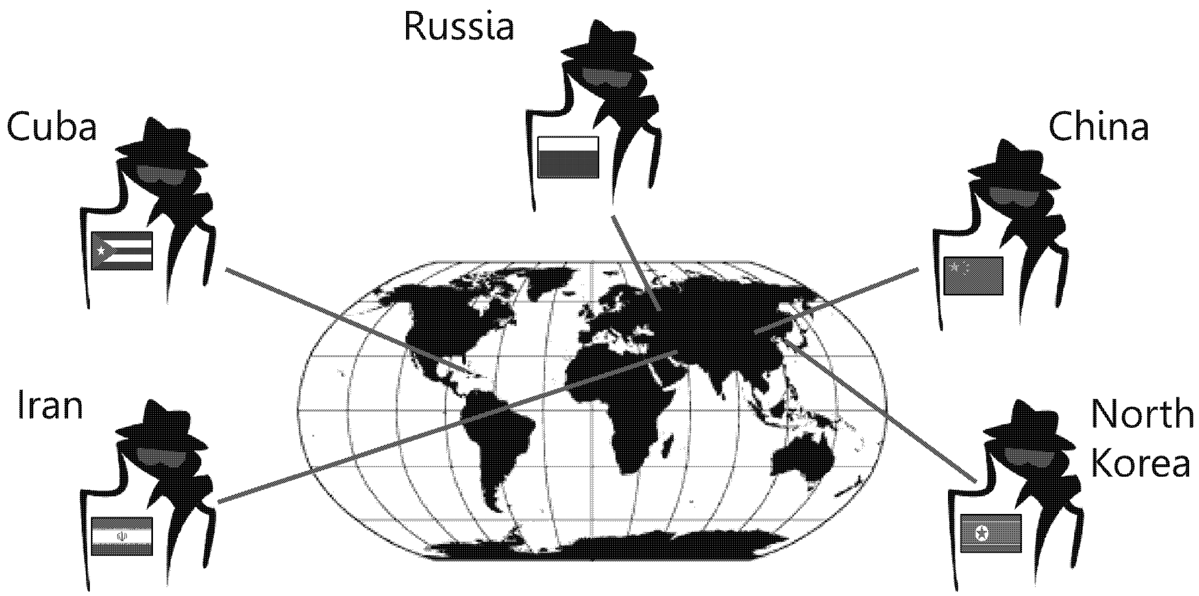
Threat Actors – Who Are They?


Cyber Criminal
Nation State
Terrorist
Lone Offender
Leaktivist
IS THIS TOMORROW
IT WASN'T LONG AFTER THE END OF THE SECOND WORLD WAR THAT COMMUNIST FORCES IN AMERICA SEIZED THEIR CHANCE. THE STORY IS SAD... THE END TRAGIC... BUT THIS IS THE WAY IT BEGAN...
Religious Cult
Corporation/
Business
Criminal Syndicate
Domestic Extremist
Violent Activist
NGO
Hacktivist



ESPIONAGE

Espionage – Nation State Threats



President Joseph R. Biden, *"Interim National Security Strategic Guidance,"* March 2021

Daniel R. Coats, *"Senate Select Committee on Intelligence Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community,"* ODNI, 29 January 2019

Growing Chinese Intelligence Threat

Espionage/Espionage-related arrests have doubled every 10 years

2010-2020 – 14
2000-2009 – 6
Pre-2000 – 3

Exploiting social networking sites for spotting, initial contact, and developing relationships

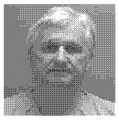
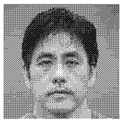
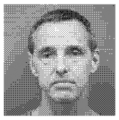
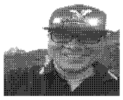
Targets are multi-gender/multi-ethnic

Money/financial gain a primary motivation/driver

Personal meetings in China

Extensive cyber operations

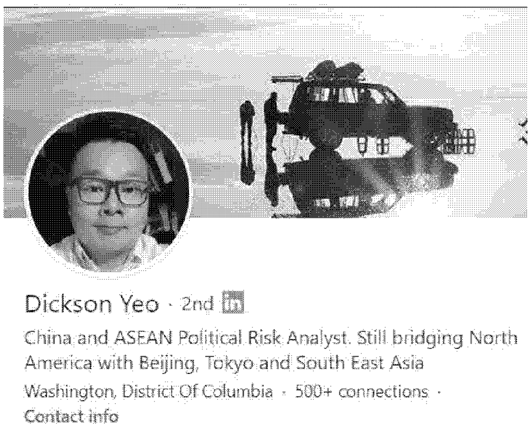
Recently Arrested Chinese Spies

Name	Years Spying	Spotted	Meetings	Motivation
Candace Claiborne USDS	2011 - 2017	China	China	Financial Blackmail
 Ron Rockwell Hansen DIA (former)	2014 - 2018	China – Printed Out LinkedIn Profiles on Colleagues for MSS	China	Financial Thrill Seeking Ego
 Jerry Chun Lee CIA (former)	2010 - 2013	China	China	Financial
 Kevin Mallory CIA/DIA (former)	2017 - 2018	LinkedIn	China	Financial
 Alexander Ma CIA (former) FBI	At least 2001 – 2010	China	China	Financial

Tell Me Your Woes

Dickson Yeo, aka, Jun Wei – Singaporean plead guilty in July 2020 for actively recruiting sources for Chinese intelligence

- Used LinkedIn to target and build contacts by using fake consulting firm (tasked by Chinese in 2018 to do so)
- "Received over 400 resumes…90% were from US Government personnel with security clearances" and he would pass more interesting ones to his Chinese intelligence officers
- Chinese handlers trained Yeo on how to elicit information from his potential targets and identify those who were "dissatisfied with work, were having financial troubles, had child support" and develop good rapport
- Relocated to WDC from January-July 2019



Dickson Yeo · 2nd in

China and ASEAN Political Risk Analyst. Still bridging North America with Beijing, Tokyo and South East Asia

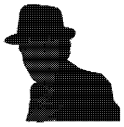
Washington, District Of Columbia · 500+ connections ·

Contact info

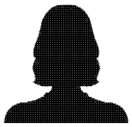
<u>Three US citizen examples</u>

- Worker on USAF F-35B with high level national security clearance – told Yeo he ***was having financial difficulties.***
- US Army officer stationed at Pentagon – told Yeo he ***was traumatized by his multiple tours in Afghanistan.*** In November 2019 tasked to turn the officer into a "permanent conduit of information."
- USDS employee – confided to Yeo he was ***dissatisfied at work and had financial difficulties***

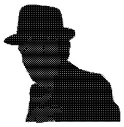
Criminal Motivation



Aws Muwafaq Abduljabber
Living in Jordan since 2010 and led efforts



Olesya Leonidovna Krasilova
Employed by US Citizenship and
Immigration Service (Aug 2011 – Feb 2019);
Worked in US Embassy in Moscow, Russia



Haithan Isa Saado Sad
Employed by US Citizenship and
Immigration Service (Nov 2007 – Jan 2016);
Worked in US Embassy in Amman, Jordan

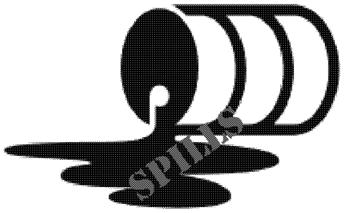
Two former US State Department employees indicted in January 2021 stealing information related to the US Refugee Admissions Program (USRAP) and, in particular, the Iraq P-2 program, which allows certain Iraqis to apply directly for refugee resettlement in the United States.

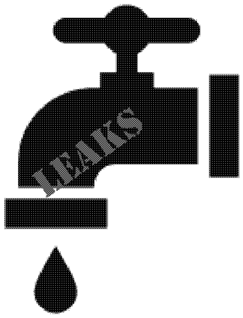
From approximately February 2016 until at least April 2019, the two stole and sold USRAP information to a Jordanian-based individual, who would use it to assist applicants in gaining admission to the United States through fraudulent means. The records contained sensitive, non-public information about refugee applicants, their family members, their employment and military history, their accounts of persecution or fear of persecution, the results of security checks, and internal assessments by US officials regarding applications.

The theft of USRAP records creates a number of risks to public safety and national security while imposing significant costs on the US Government, its taxpayers, and otherwise legitimate refugee applicants negatively impacted by the scheme.

Department of Justice, *"Former U.S. Government Employee Pleads Guilty To Conspiracy To Steal U.S. Government Records and Defraud U.S. Refugee Program,"* 26 January 2021

UNAUTHORIZED





DISCLOSURE

Unauthorized Disclosure – Spills

"Three quarters or 76% of organizations* say the biggest and most persistent security threat comes from "the enemy from within"—careless end users—who regularly clicks on bad links, placing organizations at higher risk…"

KNOWBE4, *"Security Threats and Trends Report,"* October 2019

** 600 organizations worldwide polled in mid-2019*

"Employee negligence accounted for 17 percent of all incidents in 2019…. The human risk is surpassed only by external threat actors, which accounts for 20 percent."

Security Boulevard, *"An Unexpected Insider Threat: Senior Executives Who Ignore Cybersecurity Rules,"* 20 December 2019

Cyber Criminals – Biggest Threat?

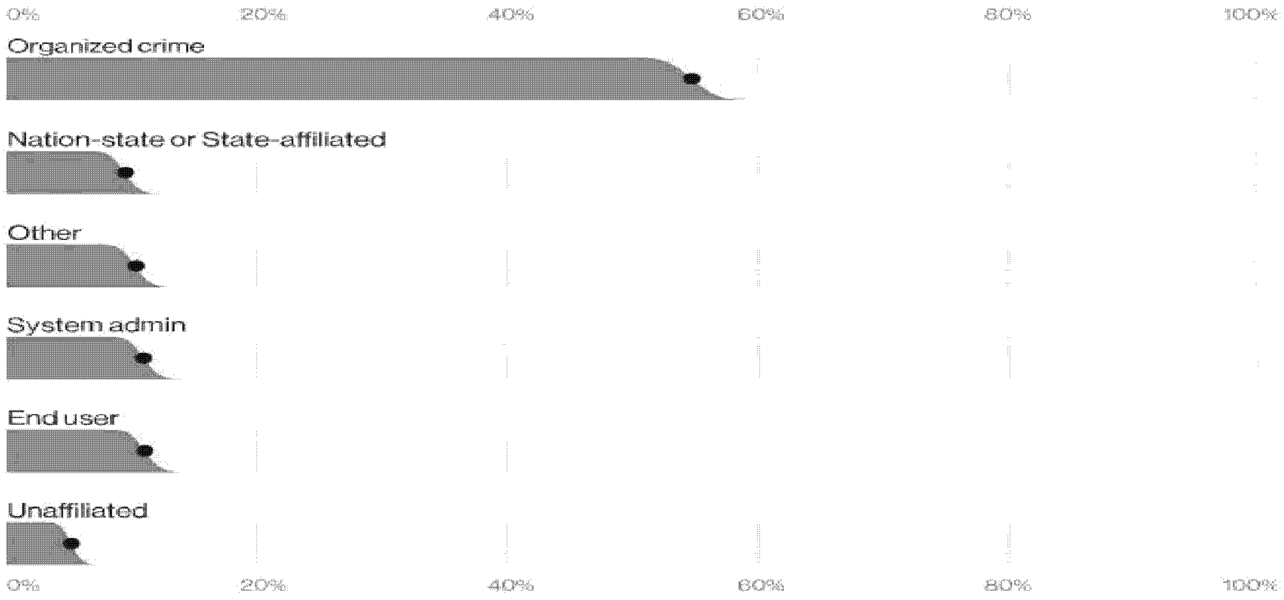


Figure 10. Top Actor varieties in breaches (n = 977)

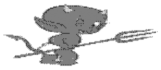
Verizon 2020 Data Breach Investigations Report

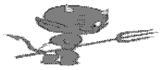
Cyber Threat Matrix

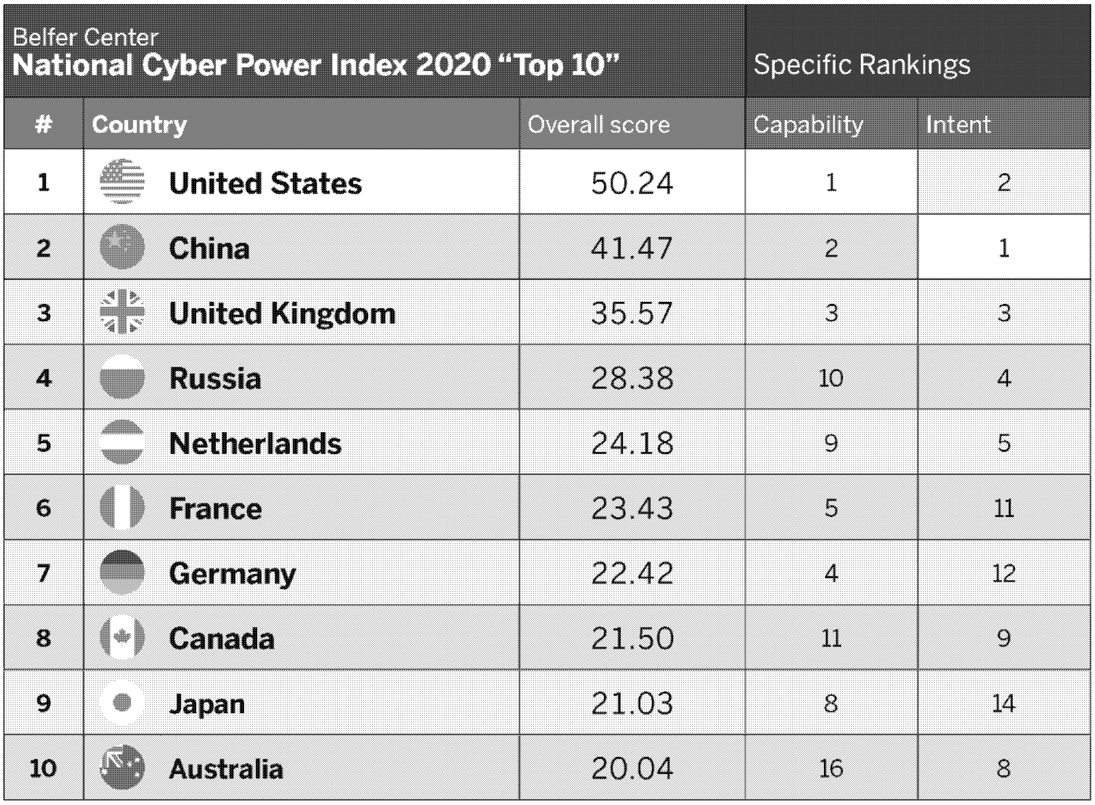
	Profit/ Financial Gain	Collection & Surveillance	Offensive Attack
Established Actors (AEs) – Those with most advanced, accurate, and agile tools. Have extensive resources—including time and money—to achieve persistence and capable of achieving global reach using advanced tradecraft.		Nation State	Nation State
Emerging Actors – Have defined processes, capabilities, and a history of targeted operations/activities but are not consistently successful to the extent of AEs. Tradecraft is limited, have beginning of organizational maturity, and are on cusp of developing products, processes, and people necessary to be AEs.	Cyber Criminal Nation State Terrorist	Nation State Terrorist	Nation State Terrorist
Opportunistic Actors – Generally associated with low-level cyber criminal activities. Market they operate in are dispersed, diverse, and segregated for tools to acquire. Are consistently innovating to keep pace with current trends and avoid law enforcement intervention.	Cyber Criminal → Can Include → Terrorist Domestic Extremist Hacktivist Violent Activist Lone Offender Religious Cult Nation State*		

Public/Private Analytic Exchange/DHS, *"Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar,"* 2019

Nation State Cyber Threat Rankings





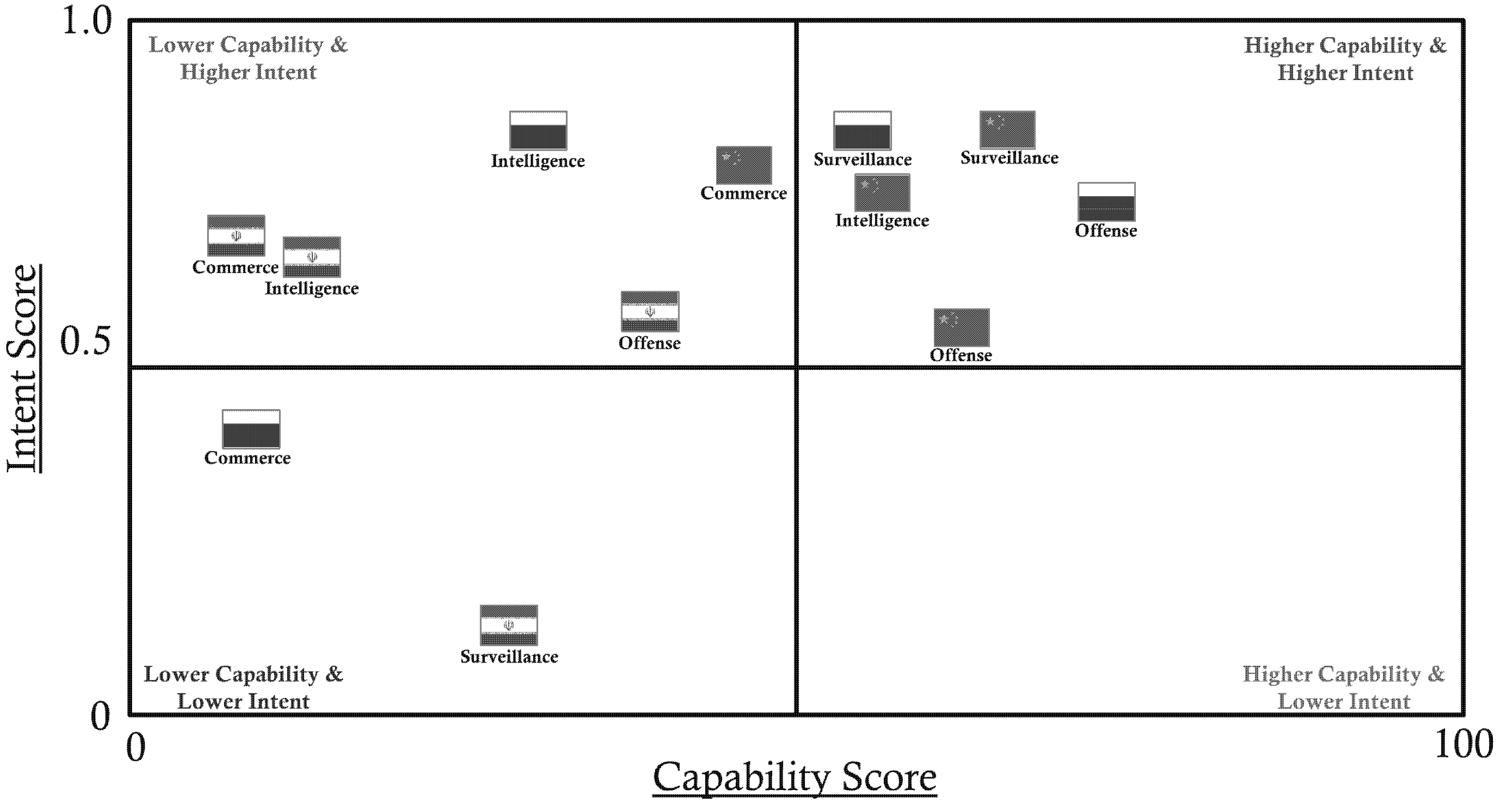


Belfer Center
National Cyber Power Index 2020 "Top 10"

#	Country	Overall score	Specific Rankings: Capability	Specific Rankings: Intent
1	**United States**	50.24	1	2
2	**China**	41.47	2	1
3	**United Kingdom**	35.57	3	3
4	**Russia**	28.38	10	4
5	**Netherlands**	24.18	9	5
6	**France**	23.43	5	11
7	**Germany**	22.42	4	12
8	**Canada**	21.50	11	9
9	**Japan**	21.03	8	14
10	**Australia**	20.04	16	8

Belfer Center for Science and International Affairs/Harvard Kennedy School, *"National Cyber Power Index 2020,"* September 2020

Quadrant Rankings for Four Nation States



Date	Major Chinese Government Breaches
???? - December 2020	Suspected Chinese hackers exploited a flaw in software made by SolarWinds Corp to help break into U.S. government computers—the **National Finance Center (NFC)**, a federal payroll agency inside the **US Department of Agriculture**, was among the affected organizations. The NFC is responsible for handling the payroll of more than 160 government agencies and includes federal employee social security numbers, phone numbers and personal email addresses as well as banking information.
April 2020	US officials reported seeing a surge of attacks by Chinese hackers against healthcare providers, pharmaceutical manufacturers, and the **US Department of Health and Human Services** amidst the COVID-19 pandemic.
December 2018	Hundreds of gigabytes of data stolen from computers of more than 45 technology companies and US Government agencies. Also stole names, SSNs, DOBs, salary info, phone numbers, and email addresses of more than 100,000 **US Navy** personnel.
September 2018	Since 2014, Starwood hotel chain network breach with estimated personal information of up to 500 million people stolen. Exposed an unusually broad array of data including names, addresses, phone numbers, passport numbers, and credit card numbers, as well as information on where people traveled and with whom.
March 2017	PII of hundreds of millions of people (potentially 143 million) stolen from Equifax, one of the credit reporting agencies that assess the financial health of nearly everyone in the United States.
May 2015	Significant amounts of customer data stolen from United Airlines.
February 2015	Anthem/Blue Cross Blue Shield hack compromised the sensitive personal information of approximately 78.8 million Americans.
April 2015	**OPM** discovered its networks infiltrated and personal information of federal employees, including security clearance information, stolen.
November 2014	**US Postal Service** computer networks breached and data of approximately 800,000 employees exfiltrated.
August 2014	**US Investigations Services** network infiltrated. One of the first steps in the 2015 OPM hack. Community Health Systems disclosed its networks infiltrated and personal information from 4.5 million patients stolen.

Nation State Cyber Operational Targeting

Country	Intelligence Collection		Offensive Operations		Crime
	Government/Military	Commercial	Physical Harm	Reputational Harm	
China	◉	◉	◎	◎	◎
Russia	◉	◎	◉	◉	◎
North Korea	◎	◎		◎	◉
Iran	◎	◎	◉	◎	◎

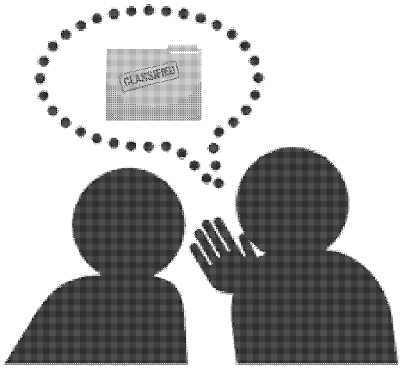
Center for Strategic and International Studies, *"Significant Cyber Incidents Since 2006,"* March 2021

Unauthorized Disclosure - Leaks

- More workers have access to more information

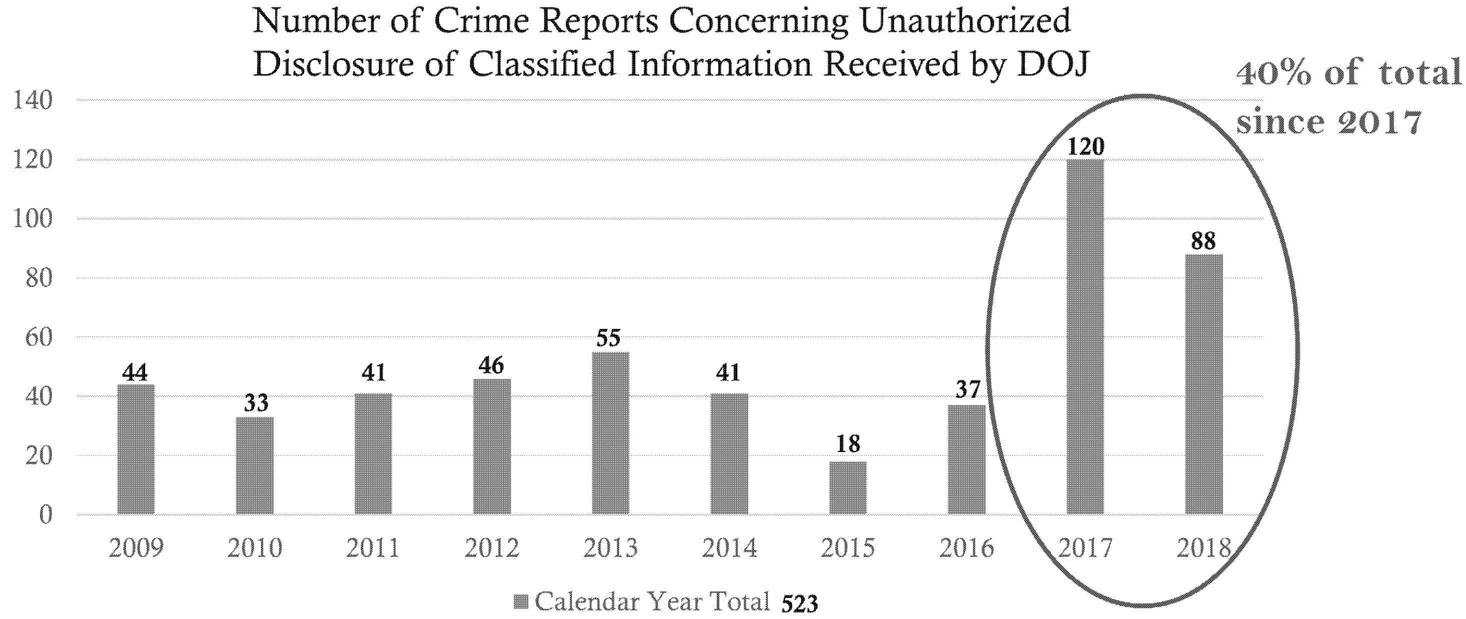
- Non-state actors pose significant threat

"Rise of the Leaktivists"



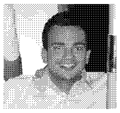
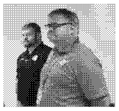
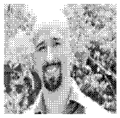
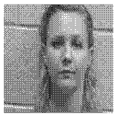
- Motivations – non-monetary/ financial (disgruntlement, ideology, ego, thrill-seeking)

Unauthorized Disclosure – Investigations

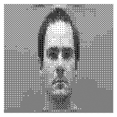
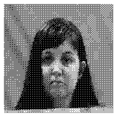
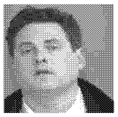


https://fas.org/irp/agency/doj/crimes-reports-2016.html
https://fas.org/irp/agency/doj/crimes-reports.html
https://fas.org/irp/agency/doj/crimes-reports-2017-18.pdf

Recent Unauthorized Disclosure (Leaks) Arrests

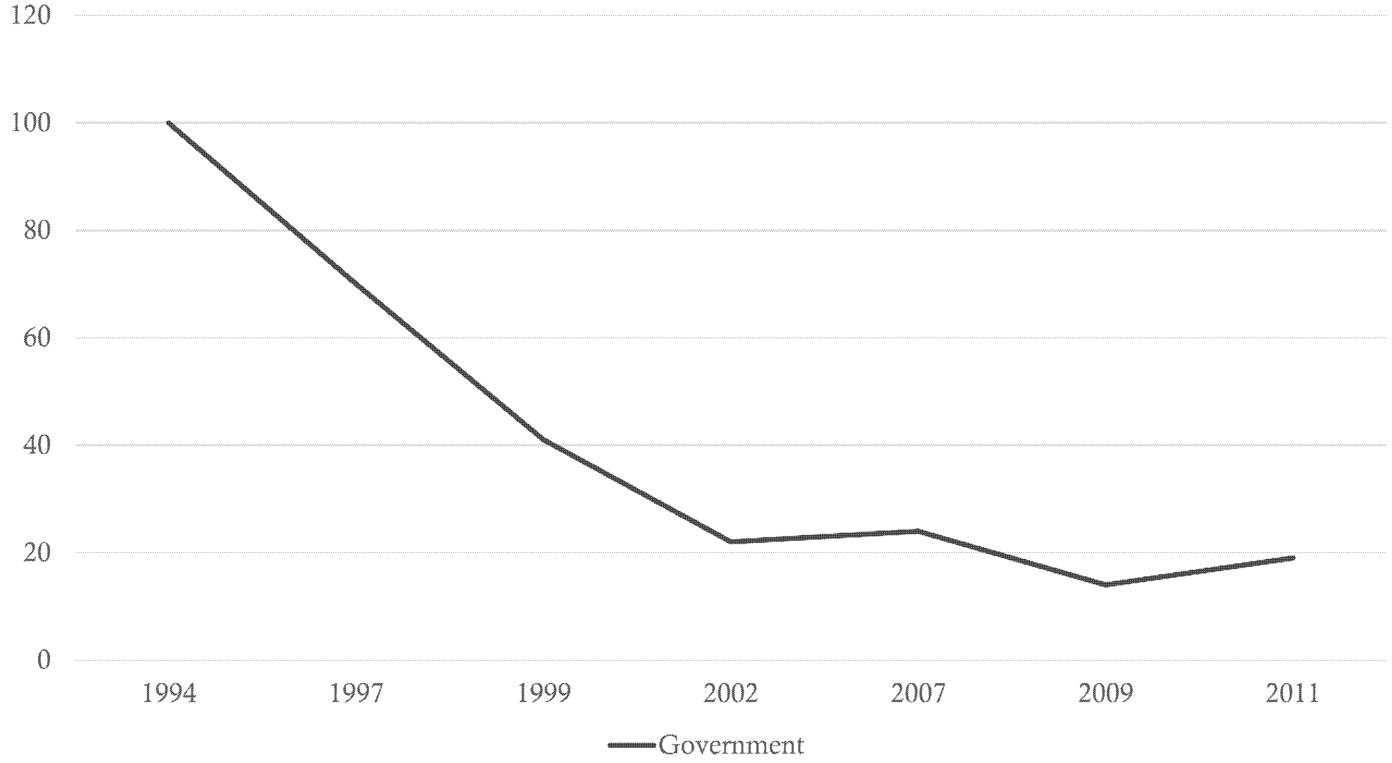
Name	Year of Activity	Provided To	Motivation
 Henry Kyle Freese DIA	2019	NBC, CNBC	Personal Relationship
 John Fry IRS	2018	Michael Avennati, The New Yorker	Political
Natalie Sours Edwards Department of Treasury	2017 - 2018	BuzzFeed	Political
 Joshua Schulte CIA (contractor)	2017	WikiLeaks	Political Disgruntlement
 Reality Winner NSA (contractor)	2017	The Intercept	Political

Other Unauthorized Disclosure Arrests

Name	Year of Activity	Provided To	Motivation
 Itzaak Vincent Kemp AFRL/NASIC (contractor)	2016 - 2019	???	???
 Elizabeth Jo Shirley NSA, ONI, DOE, DOD, NCIJTF, DOD contractors	1994 - 2002	???	Planned to offer to Russian Government officials in Mexico for help to resettle her and her daughter in Russia
 Harold Thomas Martin NSA (contractor)	~2014 - 2016	???	???

Workplace violence

Rate of nonfatal workplace violence against US Government employees, 1994-2011

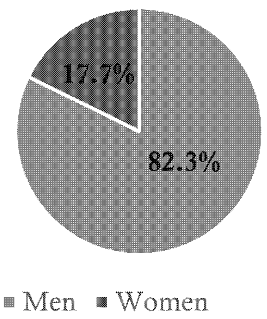


Bureau of Justice Statistics, "*Workplace Violence Against Government Employees,*" April 2013

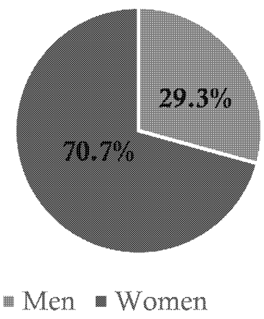
Assaults in US Workplace, 2011-2018

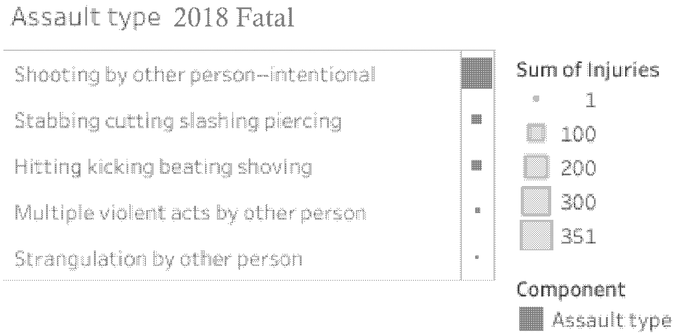
	2011	2012	2013	2014	2015	2016	2017	2018
Total	12,158	13,255	14,204	16,389	16,577	17,390	18,858	21,243
Non-fatal	11,690	12,780	13,800	15,980	16,160	16,890	18,400	20,790
Fatal	468	475	404	409	417	500	458	453

2018 Fatal



2018 Non-fatal





National Safety Council
https://injuryfacts.nsc.org/work/safety-topics/assault/

Workplace Violence Motivations

- Non-Robbery (eg, interpersonal or work-related argument) increased while Robbery decreased from 2011 - 2015

Robbery Motivation

1990s/early 2000s	65%
2015	46%

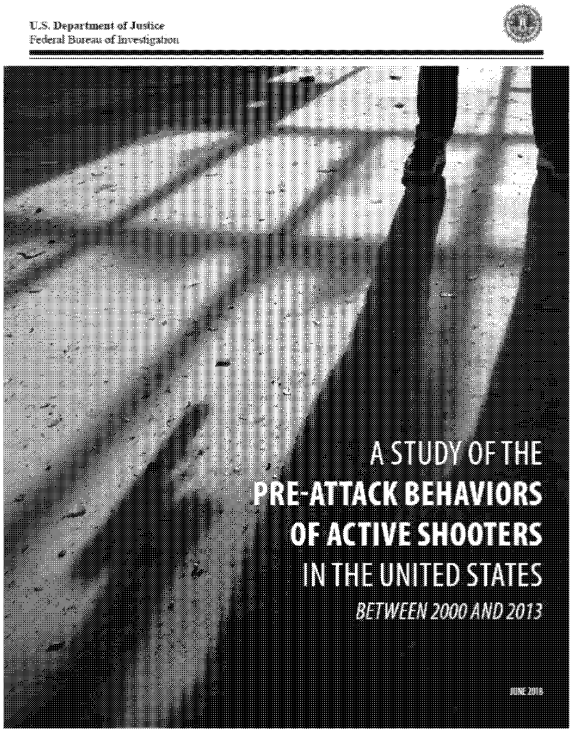
Mitchell L. Doucette, "*What Does Data Tell Us About Trends Workplace Homicides,*" Biomedcentral Blog, 19 March 2019 *https://blogs.biomedcentral.com/on-health/2019/03/19/data-tell-us-trends-workplace-homicides/*

Mitchell L. Doucette, *"Workplace Homicides Committed by Firearm: Recent Trends and Narrative Text Analysis,"* Injury Epidemiology, 18 March 2019

Pre-Attack Behaviors of Active Shooters

Key Findings:

- Active shooters were typically experiencing (an average of 3.6 separate **stressors**) in year before they attacked
- On average, each shooter displayed 4 to 5 **concerning behaviors** over time observable to others around shooter
  - Most frequent related to mental health, problematic interpersonal interactions, and leakage of violent intent
- Most common grievance were related to **adverse interpersonal or employment action** (49%)

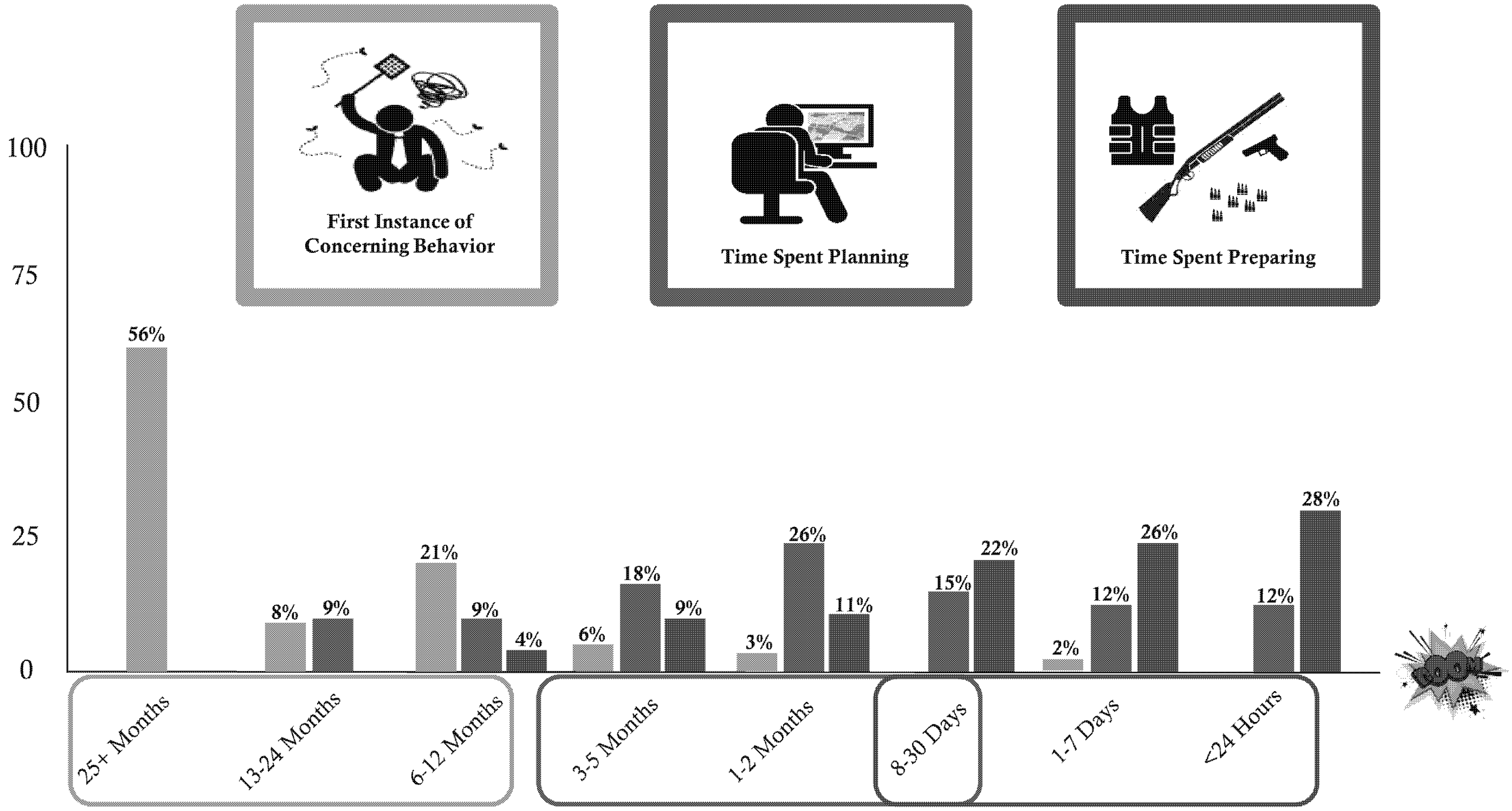


U.S. Department of Justice
Federal Bureau of Investigation

A STUDY OF THE
PRE-ATTACK BEHAVIORS
OF ACTIVE SHOOTERS
IN THE UNITED STATES
BETWEEN 2000 AND 2013

JUNE 2018

https://www.fbi.gov/file-repository/pre-attack-behaviors-of-active-shooters-in-us-2000-2013.pdf/view

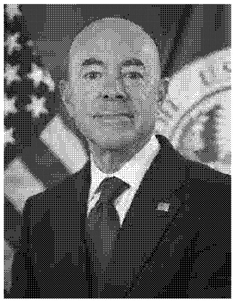

First Instance of Concerning Behavior
Time Spent Planning
Time Spent Preparing
100
75
50
25
0
56%
8%
9%
21%
9%
4%
6%
18%
9%
3%
26%
11%
15%
22%
2%
12%
26%
12%
28%
25+ Months
13-24 Months
6-12 Months
3-5 Months
1-2 Months
8-30 Days
1-7 Days
<24 Hours
BOOM

Violent Domestic Extremism

What the Big Dudes Say

"Domestic violent extremism poses the most lethal and persistent terrorism-related threat to our country today.... I have designated domestic violent extremism as a National Priority Area for the first time.... The Jan. 6 attack on the Capitol was one of many events that constitute a multi-year pattern of violence by domestic extremists."

DHS Secretary Alejandro M. Mayorkis, Washington Post, "*Opinion: Alejandro Mayorkas: How my DHS will combat domestic extremism,*" 25 February 2021



"That attack [6 January 2021 attack on the US Capitol], that siege, was criminal behavior. It is behavior that we, the FBI, view as domestic terrorism....The problem of domestic terrorism has been metastasizing across the country for a long time now and it's not going away anytime soon."

FBI Director Christopher Wray Congressional testimony, 2 March 2021

What US Government/Military Organizations Say

The IC assesses that domestic violent extremists (DVEs) who are motivated by a range of ideologies and galvanized by recent political and societal events in the United States pose an elevated threat to the Homeland in 2021.... The IC assesses that racially or ethnically motivated violent extremists (RMVEs) and militia violent extremists (MVEs) present the most lethal DVE threats, with RMVEs most likely to conduct mass-casualty attacks against civilians and MVEs typically targeting law enforcement and government personnel and facilities.

ODNI, *"Domestic Violent Extremism Poses Heightened Threat in 2021,"* 1 March 2021

"It appears the contemporary movement may be growing as antifa groups recruit followers on fears that fascism is making new inroads in the United States. Such expansion and the rising number of run-ins between antifa supporters and their opponents at public rallies raise the public profile of antifascism in the United States."

Congressional Research Service, *"Antifa—Background,"* 1 March 2018

Antigovernment extremists, specifically those tied to militias, racially or ethnically motivated, or "citing partisan political grievances will likely pose the greatest domestic terrorism threats in 2021."

FBI-DHS Joint Intelligence Bulleting, 2 March 2021

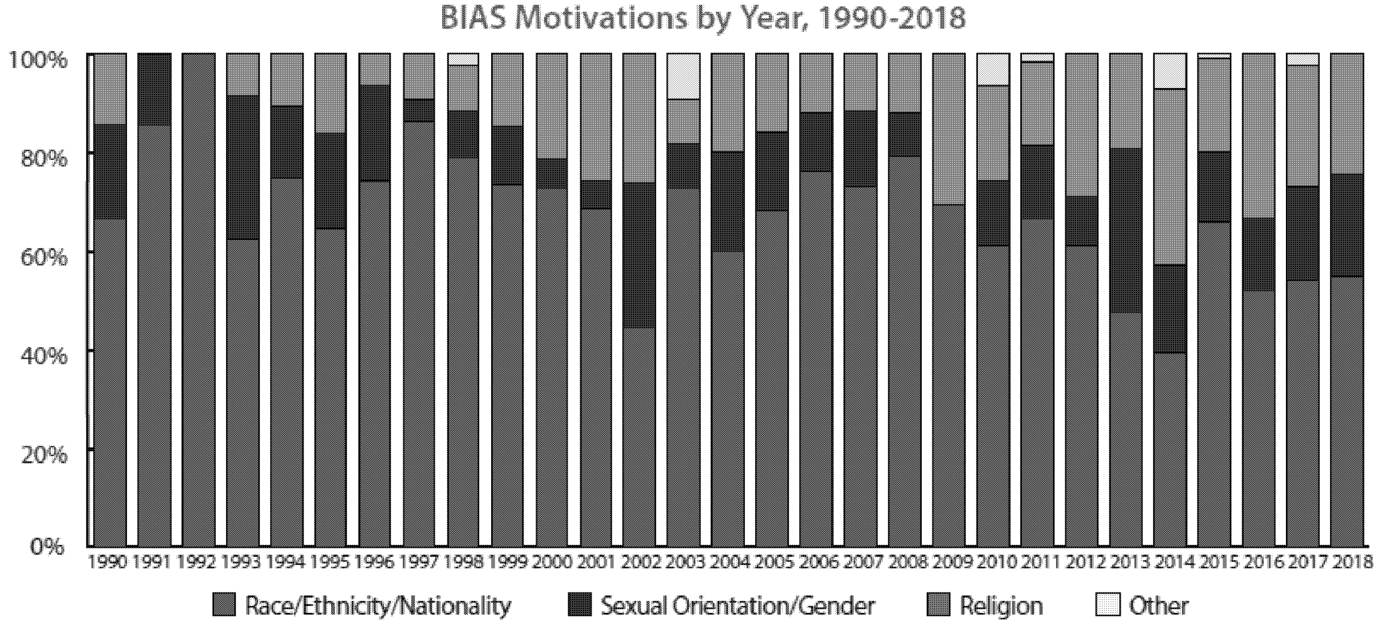
"The primary terrorist threat inside the United States will stem from lone offenders and small cells of individuals, including Domestic Violent Extremists (DVEs).... Among DVEs, racially and ethnically motivated violent extremists—specifically white supremacist extremists (WSEs)—will remain the most persistent and lethal threat in the Homeland....Another motivating force behind domestic terrorism that also poses a threat to the Homeland is anti-government/anti-authority violent extremism.

DHS Homeland Threat Assessment, October 2020

"DoD is facing a threat from domestic extremists (DE), particularly those who espouse white supremacy or white nationalist ideologies. Some domestic extremist/terror groups (a) actively attempt to recruit military personnel into their group or cause, (b) encourage their members to join the military, or (c) join, themselves, for the purpose of acquiring combat and tactical experience. Military members are highly prized by these groups as they bring legitimacy to their causes and enhance their ability to carry out attacks."

PERSEREC, *"Leveraging FBI Resources to Enhance Military Accessions Screening and Personnel Security Vetting,"* June 2020

Motivations and Characteristics of Hate Crime Offenders



"Bias towards individuals on the basis of race, ethnicity, or nationality is the most prevalent category….Offenders motivated by bias on religion and sexual orientation are the second and third most common motivations….From 2013-2018, the data show an increase in the number of offenders with these motivations."

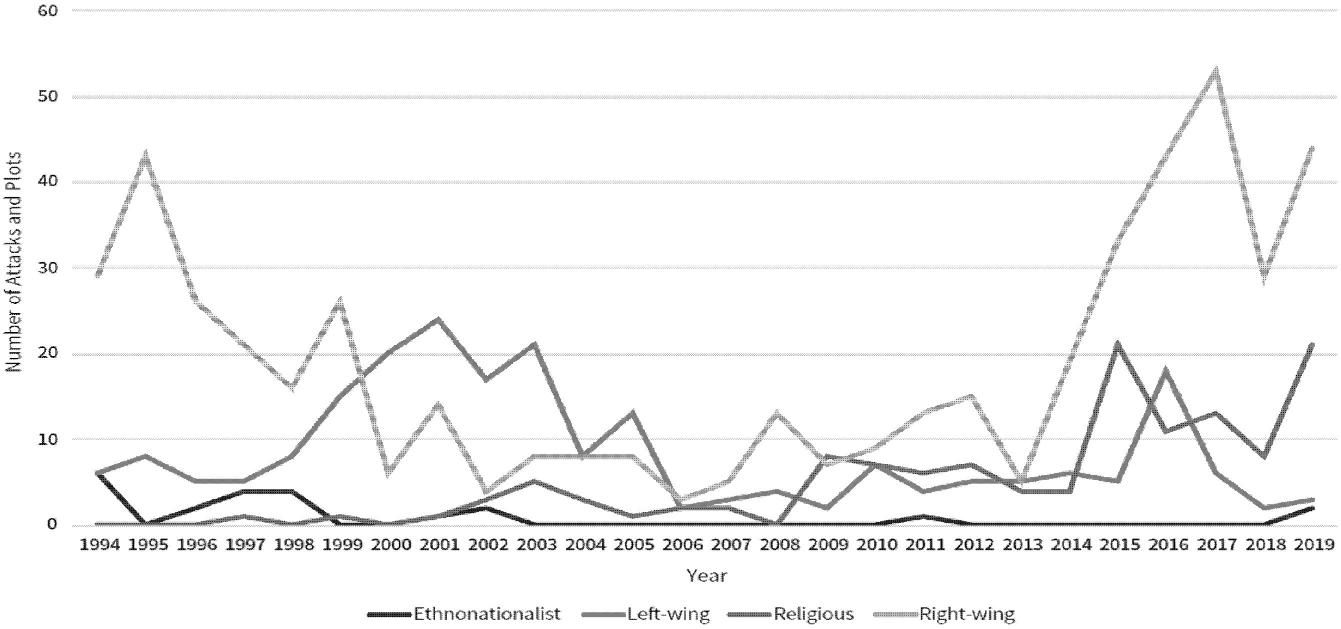
START/University of Maryland, *"Motivations and Characteristics of Hate Crime Offenders,"* October 2020

The Escalating Terrorism Problem in the United States

Center for Strategic and International Studies (CSIS)

June 2020

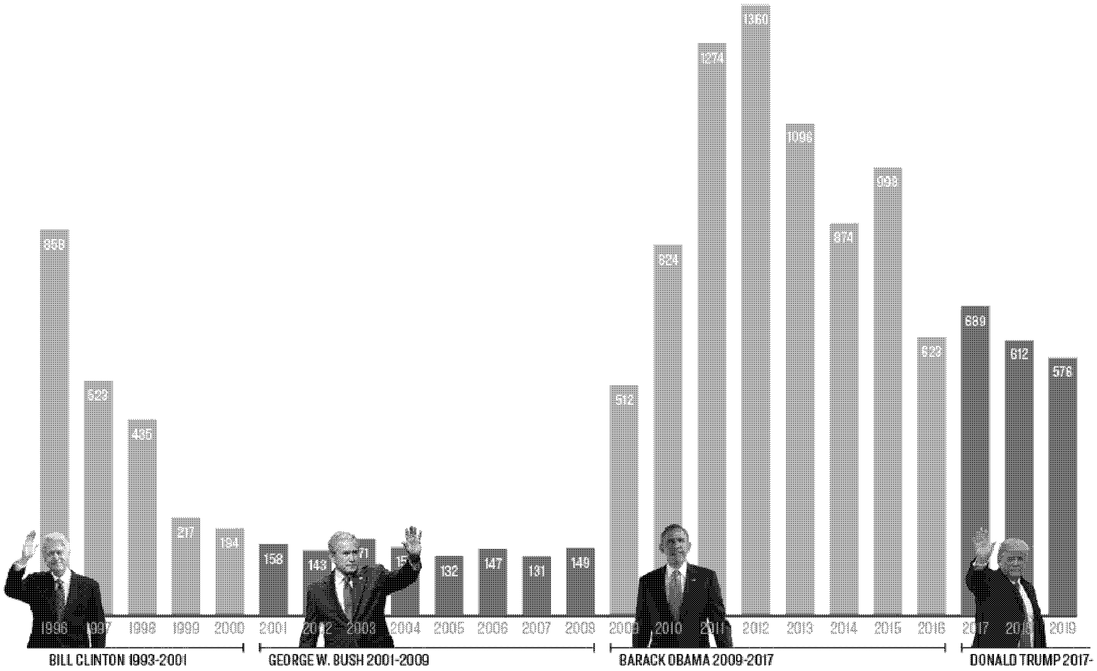
Figure 2: Number of Terrorist Attacks and Plots by Perpetrator Orientation, 1994-2019



"Between 1994 and 2020, there were 893 terrorist attacks and plots in the United States. Overall, right-wing terrorists perpetrated the majority—57 percent—of all attacks and plots during this period, compared to 25 percent committed by left-wing terrorists, 15 percent by religious terrorists, 3 percent by ethnonationalists, and 0.7 percent by terrorists with other motives."

Anti-Government Groups

ANTIGOVERNMENT 'PATRIOT' GROUPS 1995–2019

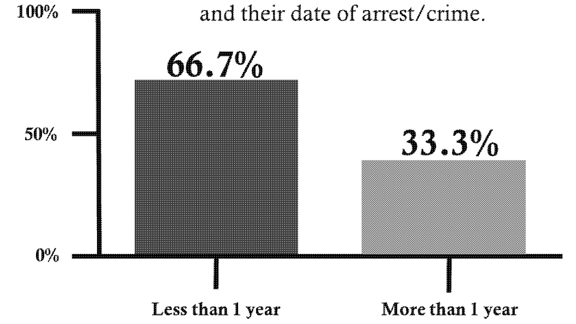


Southern Poverty Law Center
https://www.splcenter.org/fighting-hate/extremist-files/ideology/antigovernment

QAnon

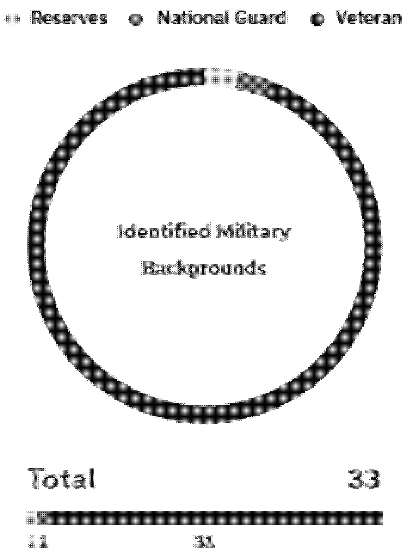
- As of 24 February 2021, 56 QAnon followers have committed ideologically-motivated crimes in the US—including 27 who have participated in the 6 January 2021 attack on the US Capitol
- Women were 19% of non-Capitol offenders and 24% of Capitol rioters
- Sixty-eight (68%) percent of non-Capitol offenders have documented mental health concerns—these include post-traumatic stress disorder, paranoid schizophrenia, bipolar disorder, and Munchausen syndrome by proxy—according to court records and other public sources
- Forty-four (44%) percent on non-Capitol offenders radicalized after experiencing a traumatic event—premature deaths of loved ones; physical, emotional, or sexual abuse; post-traumatic stress disorder from military service
    - 83% of women non-Capitol offenders experienced trauma which involved physical and/or sexual abuse of their children by a romantic partner or family member
- While some extremists radicalize over extended periods of time, data indicates the majority radicalized in less than a year, and some in mere weeks

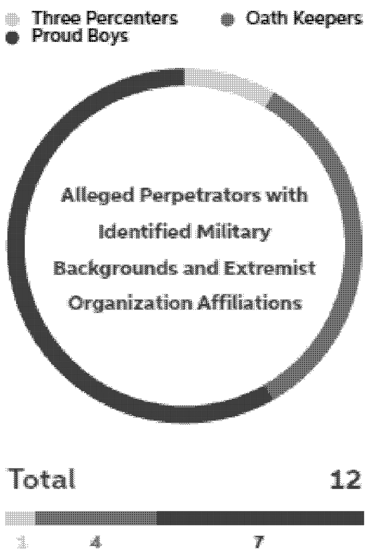
From Radicalization to Mobilization – Measured as period of time between evidence of an individual's first exposure to extremist views and their date of arrest/crime.



START/University of Maryland, *"QAnon Offenders in the United States,"* February 2021

Extremists Involved in 6 January 2021 Attack on the Capitol with Ties to US Military

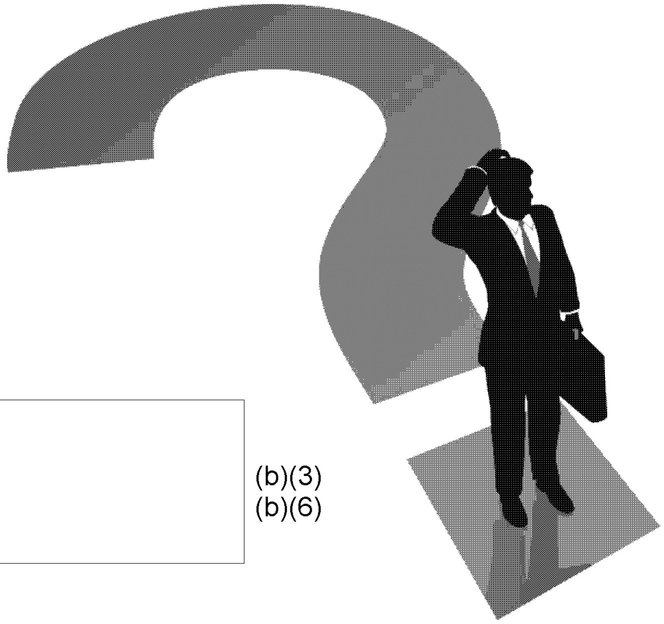




"…33 individuals with military backgrounds. These included 31 veterans, 1 current member of the National Guard, and 1 current member of the Army Reserves. 36% of individuals with military backgrounds also had concrete ties to various extremist organizations, including the Proud Boys (7), Oath Keepers (4), and Three Percenters (1)."

George Washington University, *"'This is Our House!' A Preliminary Assessment of the Capitol Hill Siege Participants,"* March 2021

Questions?



[redacted] (b)(3)
(b)(6)

DEPARTMENT OF JUSTICE

Insider Threat Trends

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Updated 10 June 2021

Objectives

1. Discuss current trends in Workplace Violence

2. Discuss current trends in Domestic Violent Extremism

3. Discuss current trends in Espionage

4. Discuss current trends in Unauthorized Disclosure

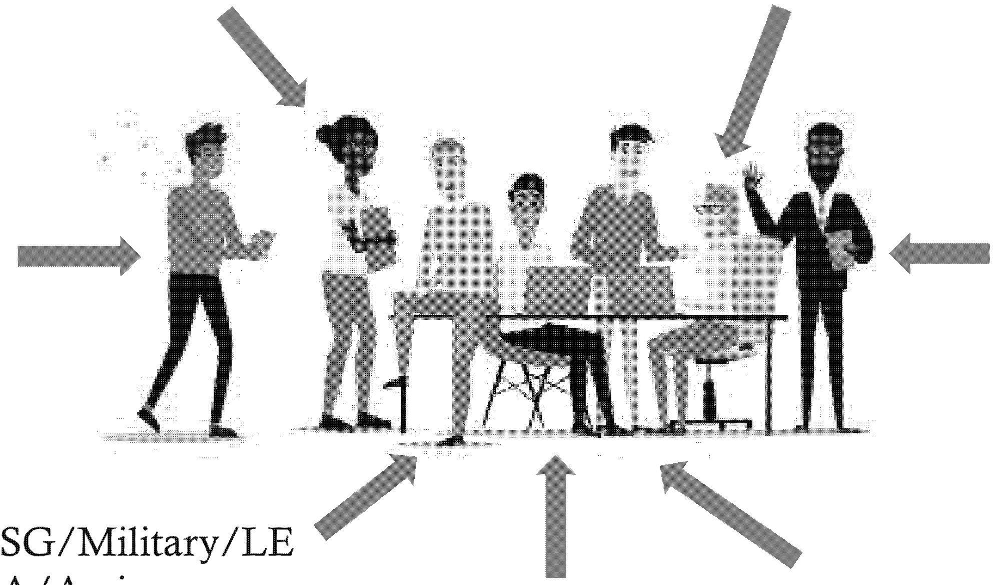
Key Assumptions

1. Population of US Federal Government/US Military personnel mirror US population

2. Major insider threat event is a rare occurrence – based on low number of reported incidents over the years

3. Risk of a major insider threat event is growing – based on larger number of threat actors, and increased opportunity and vulnerabilities compared to past years

Who Can be an "Insider?"



Contract Employee

Foreign National

Vendor

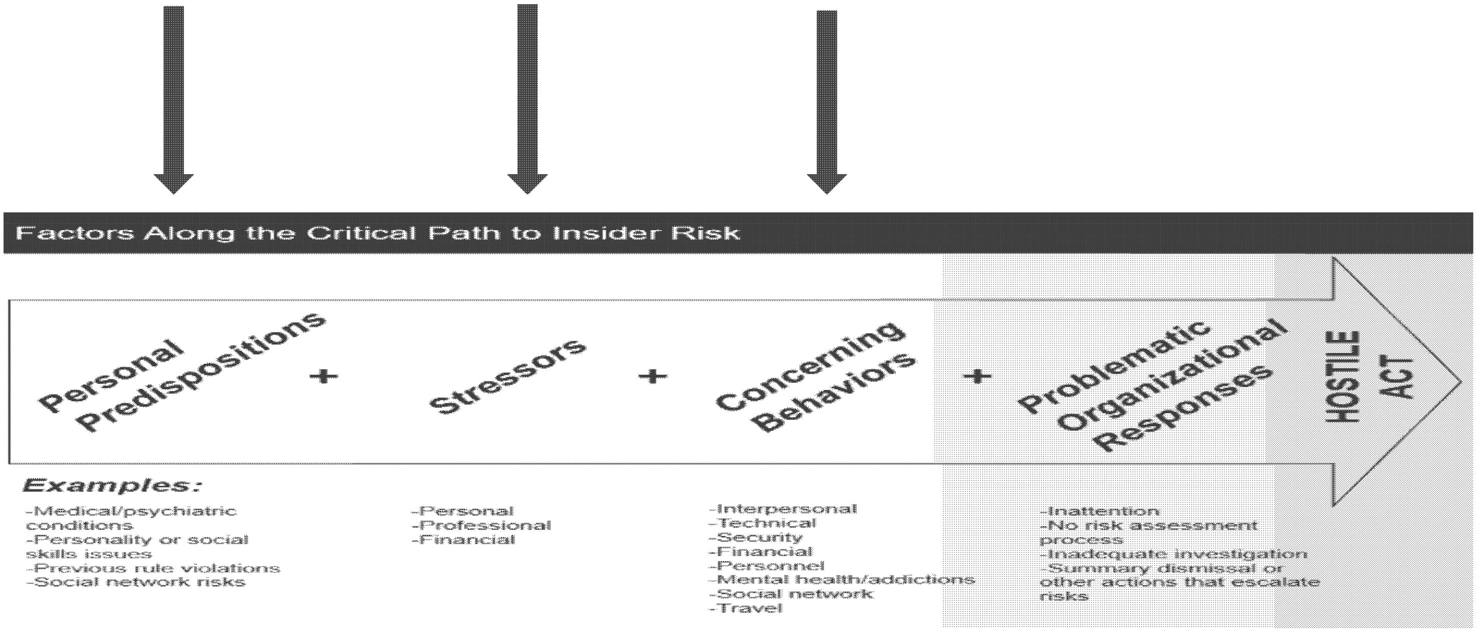
Direct Employee

OC – USG/Military/LE
JDA/Assignee

Outside Colleague
(OC)

OC – Non-USG/Military/LE
(Private Sector/Academia)

Key Indicator – Mental Health



Factors Along the Critical Path to Insider Risk

Personal Predispositions + Stressors + Concerning Behaviors + Problematic Organizational Responses → HOSTILE ACT

Examples:

Personal Predispositions:
-Medical/psychiatric conditions
-Personality or social skills issues
-Previous rule violations
-Social network risks

Stressors:
-Personal
-Professional
-Financial

Concerning Behaviors:
-Interpersonal
-Technical
-Security
-Financial
-Personnel
-Mental health/addictions
-Social network
-Travel

Problematic Organizational Responses:
-Inattention
-No risk assessment process
-Inadequate investigation
-Summary dismissal or other actions that escalate risks

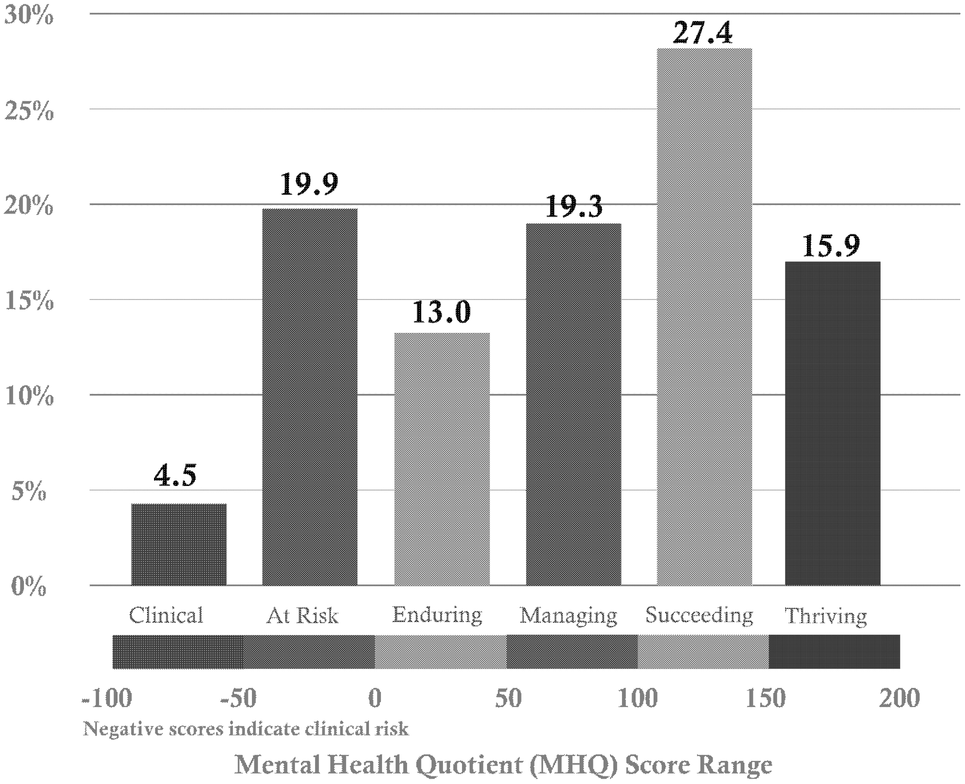
Eric Shaw and Laura Sellers, *"Application of the Critical-Path Method to Evaluate Insider Risks,"* CIA Studies in Intelligence, June 2015

Key Indicator – Mental Health

Approximately 25% of the US population have or are at risk for clinical mental health challenges

Age Group	Percentage at ● Clinical or ● At Risk
18-24	46.5
25-44	33.0
45-64	19.8

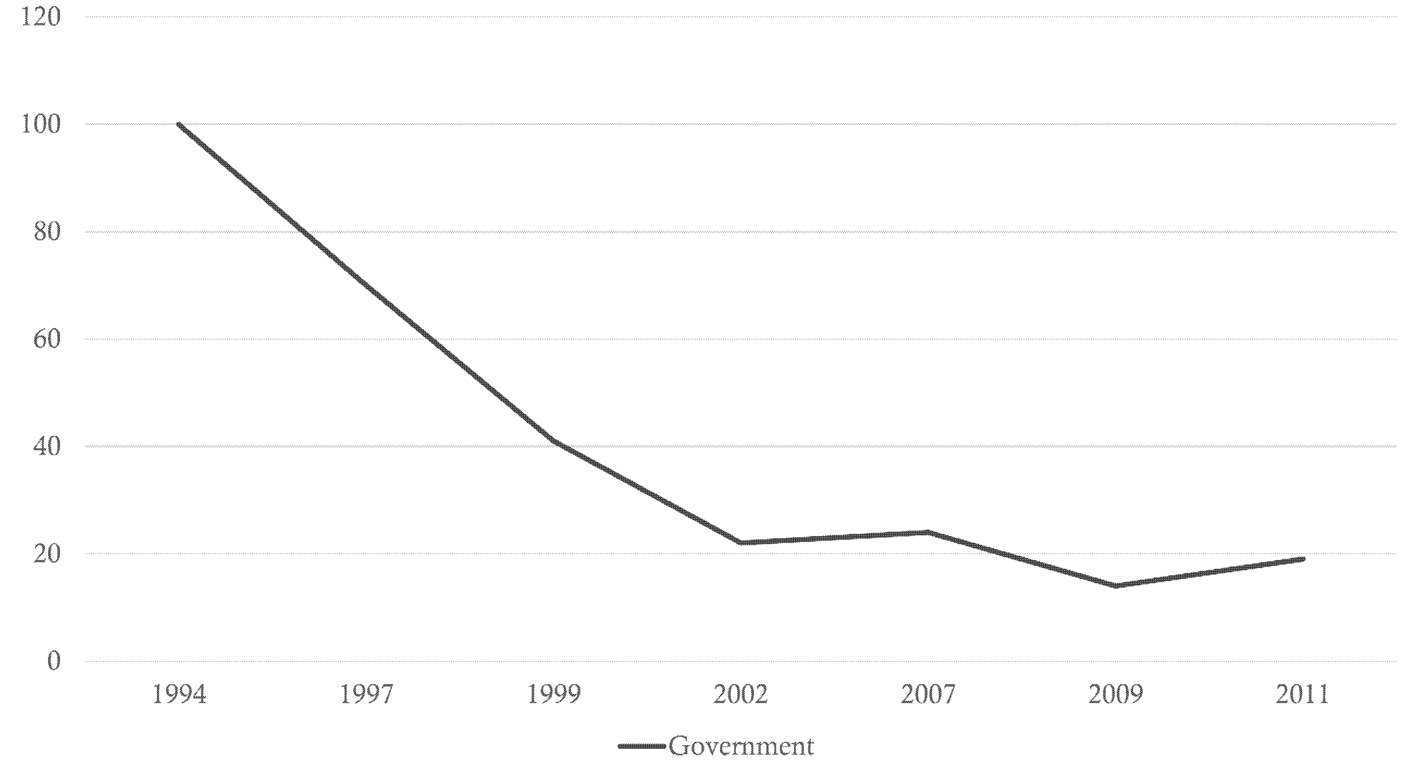
Almost half of 18-24, one-third of 25-44, and one-fifth of 45-64 have or are at risk for clinical mental health challenges



Sapien Labs, *"Mental State of the World 2020,"* 9 June 2021

Workplace violence

Rate of nonfatal workplace violence against US Government employees, 1994-2011

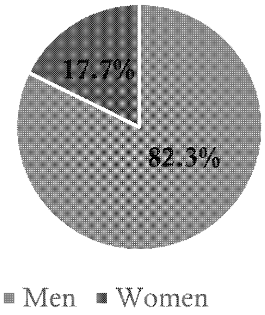


Bureau of Justice Statistics, "*Workplace Violence Against Government Employees,"* April 2013

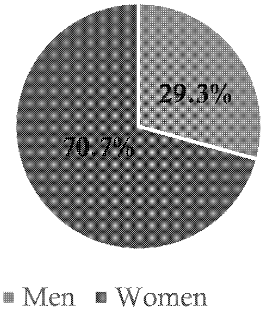
Assaults in US Workplace, 2011-2018

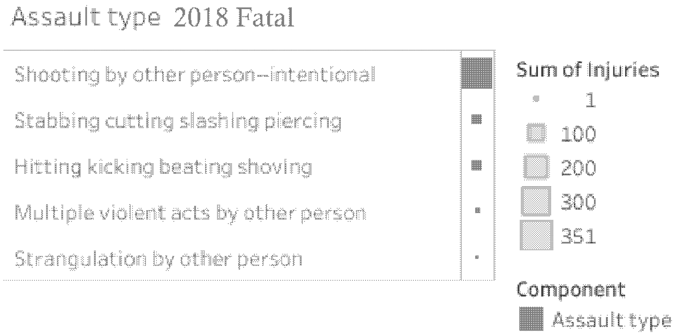
	2011	2012	2013	2014	2015	2016	2017	2018
Total	12,158	13,255	14,204	16,389	16,577	17,390	18,858	21,243
Non-fatal	11,690	12,780	13,800	15,980	16,160	16,890	18,400	20,790
Fatal	468	475	404	409	417	500	458	453

2018 Fatal



2018 Non-fatal





National Safety Council
https://injuryfacts.nsc.org/work/safety-topics/assault/

Workplace Violence Motivations

- Non-Robbery (eg, interpersonal or work-related argument) increased while Robbery decreased from 2011 - 2015

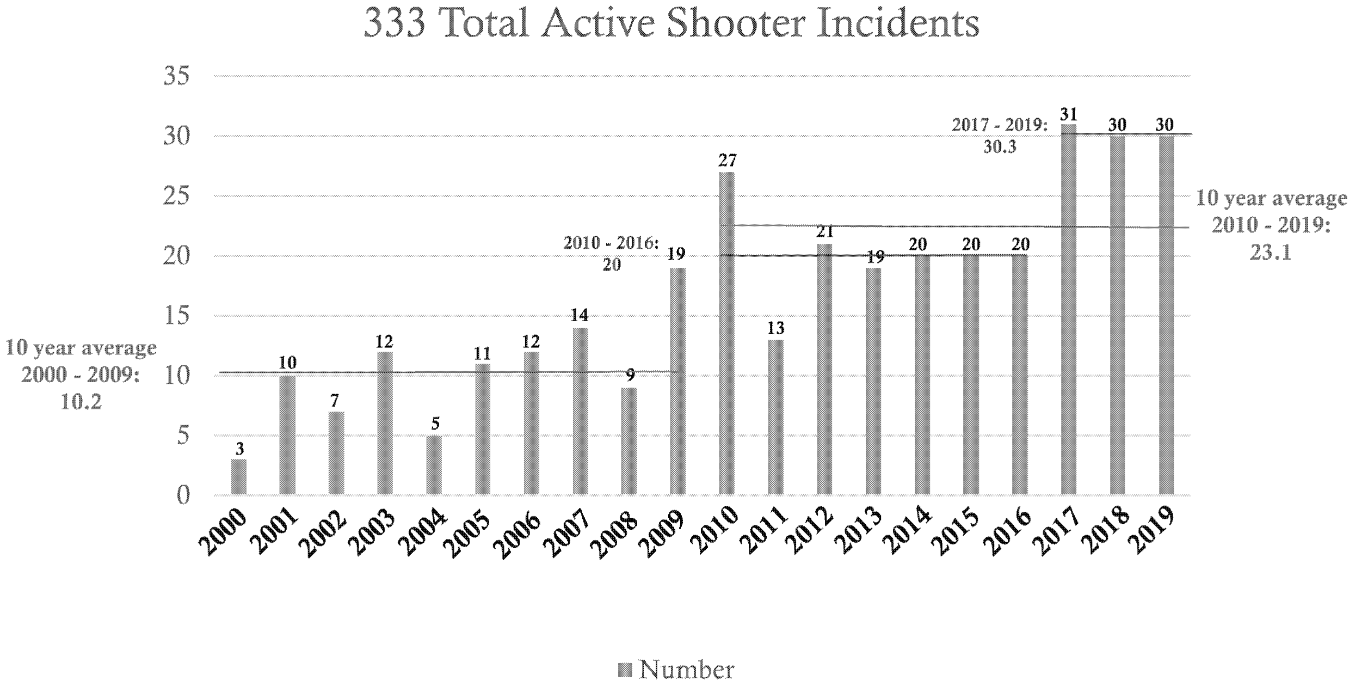
Robbery Motivation

1990s/early 2000s	65%
2015	46%

Mitchell L. Doucette, "*What Does Data Tell Us About Trends Workplace Homicides,*" Biomedcentral Blog, 19 March 2019
https://blogs.biomedcentral.com/on-health/2019/03/19/data-tell-us-trends-workplace-homicides/

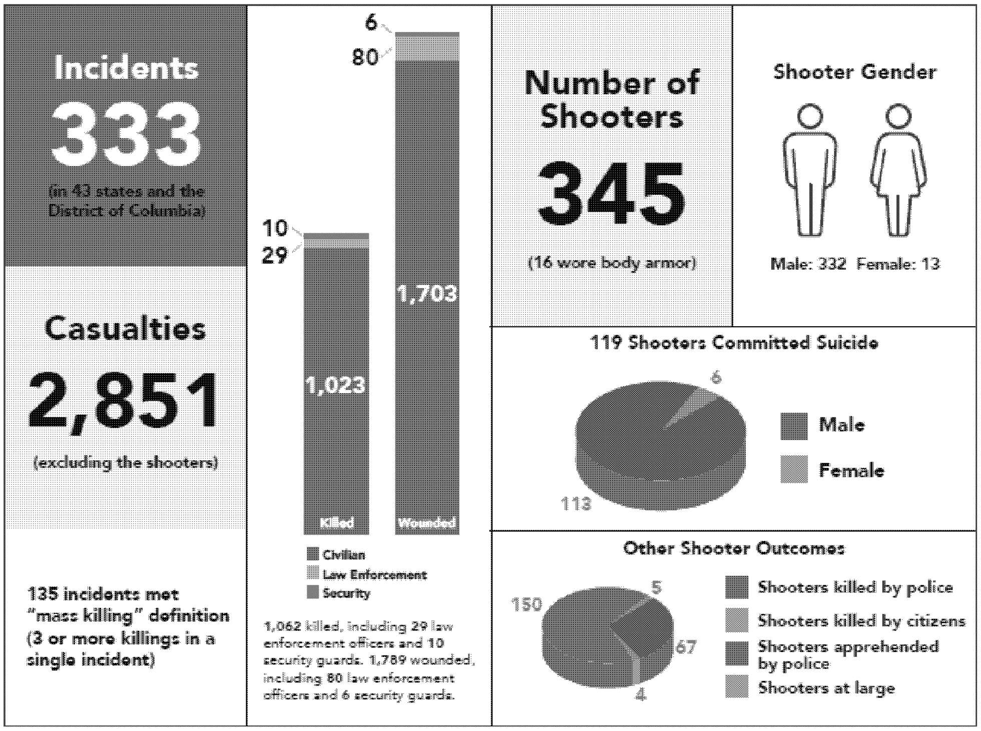
Mitchell L. Doucette, *"Workplace Homicides Committed by Firearm: Recent Trends and Narrative Text Analysis,"* Injury Epidemiology, 18 March 2019

Active Shooters: 2000 - 2019



FBI, "Active Shooter Incidents 20-Year Review 2000-2019," May 2021

20-Year Active Shooter Summary



135 incidents met "mass killing" definition (3 or more killings in a single incident)

1,062 killed, including 29 law enforcement officers and 10 security guards. 1,789 wounded, including 80 law enforcement officers and 6 security guards.

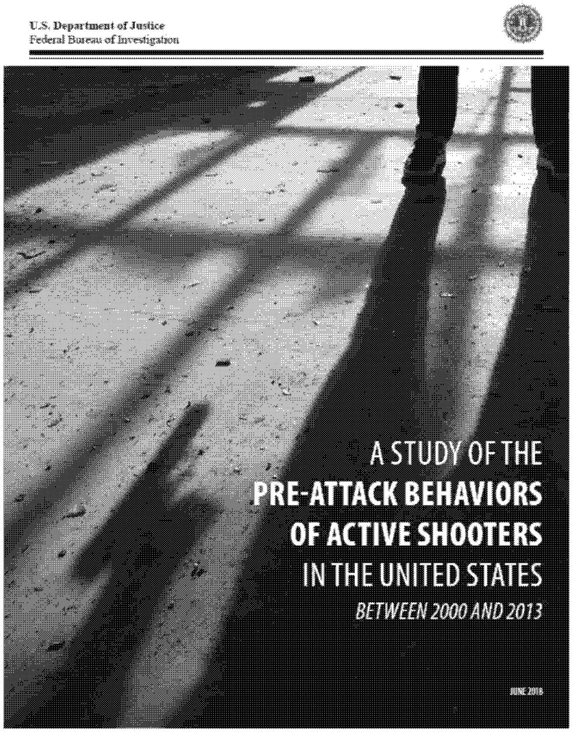
Incidents: 333 (in 43 states and the District of Columbia). Total casualties: 2,851 (excluding the shooters). 135 incidents met "mass killing" definition (3 or more killings in a single incident). Killed: 1,062 (including 1,023 civilians, 29 law enforcement officers and 10 security guards). Wounded: 1,789 (including 1,703 civilians, 80 law enforcement officers, and 6 security guards). Number of shooters: 345 (16 wore body armor). Shooter gender: 332 male, 13 female. 119 shooters committed suicide (113 male, 6 female). Other shooter outcomes: 67 killed by police, 4 killed by citizens, 150 apprehended by police, 4 at large.

FBI, "Active Shooter Incidents 20-Year Review 2000-2019," May 2021

Pre-Attack Behaviors of Active Shooters

Key Findings:

- Active shooters were typically experiencing (an average of 3.6 separate stressors) in year before they attacked
- On average, each shooter displayed 4 to 5 concerning behaviors over time observable to others around shooter
    - Most frequent related to mental health, problematic interpersonal interactions, and leakage of violent intent
- Most common grievance were related to adverse interpersonal or employment action (49%)

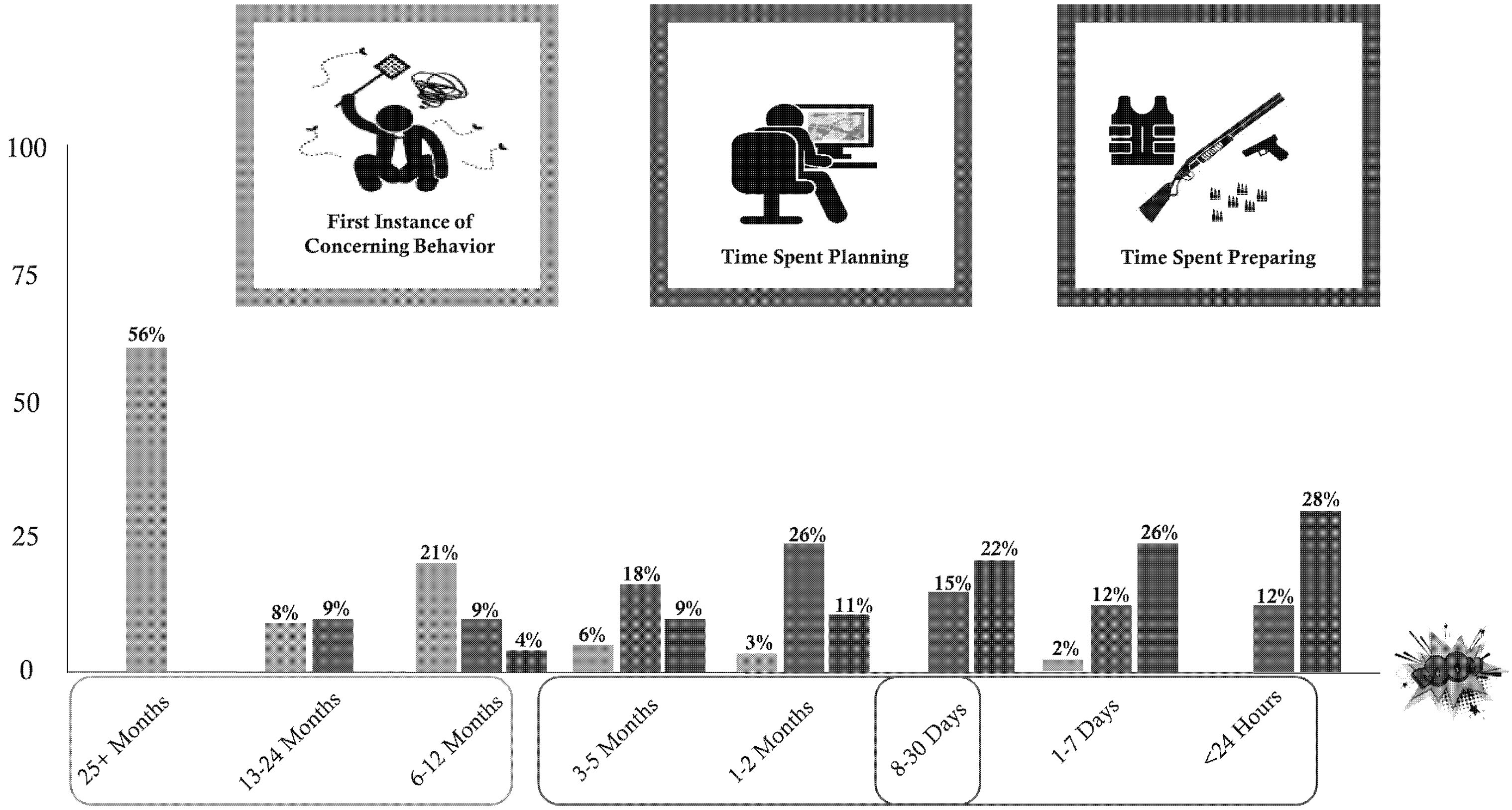


U.S. Department of Justice
Federal Bureau of Investigation

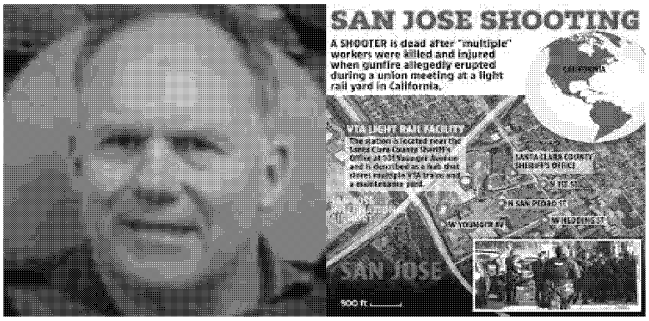
A STUDY OF THE
PRE-ATTACK BEHAVIORS
OF ACTIVE SHOOTERS
IN THE UNITED STATES
BETWEEN 2000 AND 2013

JUNE 2018

https://www.fbi.gov/file-repository/pre-attack-behaviors-of-active-shooters-in-us-2000-2013.pdf/view


First Instance of Concerning Behavior
Time Spent Planning
Time Spent Preparing
100
75
50
25
0
56%
8%
9%
21%
9%
4%
6%
18%
9%
3%
26%
11%
15%
22%
2%
12%
26%
12%
28%
25+ Months
13-24 Months
6-12 Months
3-5 Months
1-2 Months
8-30 Days
1-7 Days
<24 Hours
BOOM

26 May 2021


SAN JOSE SHOOTING
A SHOOTER is dead after "multiple" workers were killed and injured when gunfire allegedly erupted during a union meeting at a light rail yard in California.
CALIFORNIA
VTA LIGHT RAIL FACILITY
SANTA CLARA COUNTY SHERIFF'S OFFICE
N 1ST ST
N SAN PEDRO ST
W YOUNGER AV
W HEDDING ST
SAN JOSE
900 ft

Samuel Cassidy – San Jose Shooter

https://sanfrancisco.cbslocal.com/2021/05/29/samuel-cassidy-gunman-vta-rail-yard-san-jose/

https://www.the-sun.com/news/2968767/meet-samuel-cassidys-ex-wife-cecilia-nelms/

- 8 Aug 2016 – CBP detains/questions Cassidy on return trip from the Philippines: possessed "books about terrorism and fear and manifestos…as well as a black memo book filled with lots of notes about he hates the VTA [his employer]."
- Pre-2005 – ex-wife said he talked about killing people at work and would return from work angry/resentful over assignments he perceived as unfair.
- 2009 court filing – ex-girlfriend said Cassidy had bipolar disorder, sexually assaulted her, and had "major mood swings" exacerbated when he consumed large amounts of alcohol.
- Co-worker said Cassidy stuck out as a loner and outsider. Ex-wife said he was uncomfortable around people.
- Sheriff's officials described Cassidy as "highly disgruntled VTA employee for many years."
- Ex-girlfriend in court filing: suggests Cassidy admitted he stole tools and equipment from VTA and previous employer.

4 December 2019

OAHU
USS Arizona memorial
Ford Island
USS Missouri
Joint Base Pearl Harbor-Hickam
Three killed in Pearl Harbor shooting
Hickam Field
Daniel K. Inouye International Airport

SOURCE ESRI; maps4news.com/©HERE; USA TODAY

Gabriel Romero– Pearl Harbor Naval Base Shooter

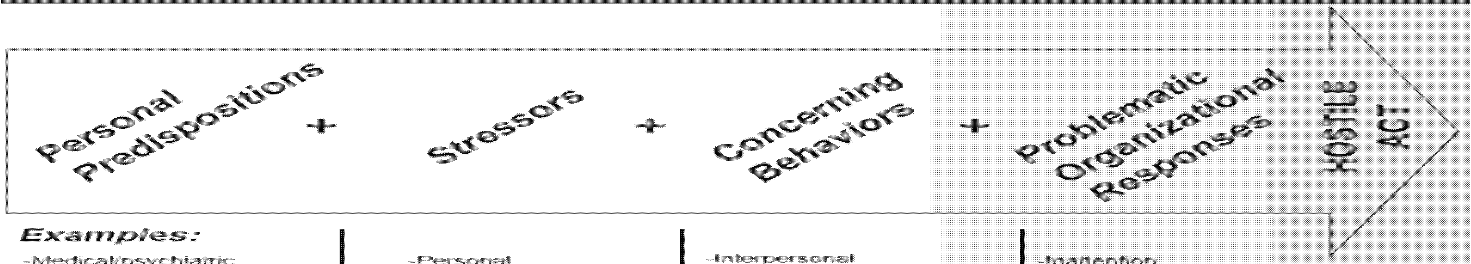
https://www.navytimes.com/news/your-navy/2020/09/29/a-troubled-sailor-was-underdiagnosed-by-mental-health-officials-before-mass-shooting/

https://www.secnav.navy.mil/foia/readingroom/HotTopics/PHNSY%20INV/PHNSY%20INV%20-%20FINAL%20REPORT%20and%20Endorsement%20(Redacted%20for%20Release).pdf

- Circa April 2019 – Fell behind qualifications for his submarine and chain of command took administrative action to address exceeding the qualifications deadline, poor performance, and continued tardiness.
- Aug/Sep 2019 – Reacted angrily and yelled when a shipmate suggested counseling support when Romero appeared stressed.
- June – November 2019 – Counselled in writing or received extra military instructions 10x for poor work performance and being late.
- June 2019 – beginning this month had to attend after-work study periods for his qualifications delinquency.
- Cried during several encounters/counseling sessions (May/Jun 2019, 21 & 26 Nov 2019, 3 Dec 2019).
- Told he failed to advance in paygrade (26 Nov 2019), would be referred to CO's non-judicial punishment if he was late again (3 Dec 2019).
- Told his mother, fellow colleague, mental health (eMHP) staff, and wrote in his personal journal he felt alienated from shipmates, a hostile work environment, and frustration with his work.
- Beginning in Sep 2019 – went to eMPH for eight (8) visits.
- Involved in two motor vehicle accidents (Dec 2018 and Nov 2019).
- Possible mental health issues reported:
    - 4 Mar 2019 – difficulty focusing at traffic court hearing; medical center emergency room personnel noted possible Attention Deficit Disorder and referred him to eMHP.
    - 19 Sep 2019 – Division Chief noticed Romero upset about his declining mental health and would not express himself to his chief.
    - 23 Sep 2019 – eMHP psychologist diagnosed "Phase of Life Problem" and an "Unspecified Problem Related to Unspecified Psychosocial Circumstances." Recommended continued individual therapy to focus on issues related to family matters, failing health, and teach Romero coping skills.

Shaw's Critical Path - Cassidy

Factors Along the Critical Path to Insider Risk



Examples:

-Medical/psychiatric conditions
-Personality or social skills issues
-Previous rule violations
-Social network risks

Co-worker: Cassidy is a loner and outsider Ex-wife: Cassidy uncomfortable around people.

Ex-girlfriend: "mood swings"/bipolar disorder

Ex-girlfriend: "mood swings" exacerbated by drinking a lot

-Personal
-Professional
-Financial

Ex-wife: returns from work angry/resentful over assignments

Sheriff's officials: Highly disgruntled VTA employee for many years

-Interpersonal
-Technical
-Security
-Financial
-Personnel
-Mental health/addictions
-Social network
-Travel

Books on terrorism and fear and manifestos

Black memo – hates VTA

Tells ex-wife about killing people at work

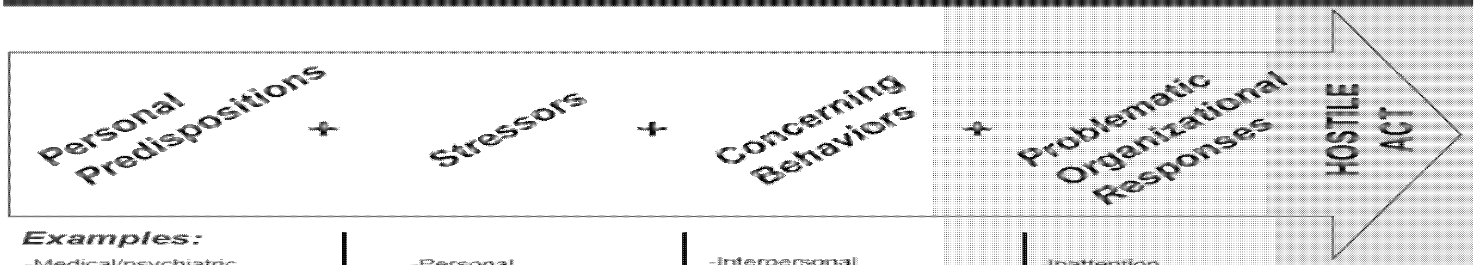
Ex-girlfriend: Cassidy sexually assaulted her

Ex-girlfriend: Cassidy admits he stole tools /equipment from VTA and previous employer

-Inattention
-No risk assessment process
-Inadequate investigation
-Summary dismissal or other actions that escalate risks

Shaw's Critical Path - Romero

Factors Along the Critical Path to Insider Risk



Examples:

-Medical/psychiatric conditions
-Personality or social skills issues
-Previous rule violations
-Social network risks

Expresses alienation from shipmates

Two motor vehicle accidents within a year

First expression of focusing issues and possible ADD

Mental health visits

Upset about his declining mental health/ not expressing himself to his chief

Family issues, failing health, being taught coping skills

-Personal
-Professional
-Financial

Work Performance Issues

Cries during several encounters

Fails to advance and possible referral to CO NJP

Claims hostile work environment

Says frustrated with his work

-Interpersonal
-Technical
-Security
-Financial
-Personnel
-Mental health/addictions
-Social network
-Travel

Becomes angry/yells when shipmate recommends counseling for stress

Cries during several encounters

Expresses alienation from shipmates

Claims hostile work environment

Upset about his declining mental health/ not expressing himself to his chief

-Inattention
-No risk assessment process
-Inadequate investigation
-Summary dismissal or other actions that escalate risks

<u>Indicators not seen:</u>

- **Never diagnosed with a mental disorder**
- **Never made any known homicidal/suicidal ideations**
- **No criminal record**
- **No history of alcohol or drug abuse, financial problems, weapons mishandling, or known interest in previous shooting incidents**
- **No prior history of violence or threatening violence**

Violent Domestic Extremism

What US Government/Military Organizations Say

The IC assesses that domestic violent extremists (DVEs) who are motivated by a range of ideologies and galvanized by recent political and societal events in the United States pose an elevated threat to the Homeland in 2021…. The IC assesses that racially or ethnically motivated violent extremists (RMVEs) and militia violent extremists (MVEs) present the most lethal DVE threats, with RMVEs most likely to conduct mass-casualty attacks against civilians and MVEs typically targeting law enforcement and government personnel and facilities.

ODNI, *"Domestic Violent Extremism Poses Heightened Threat in 2021,"* 1 March 2021

"It appears the contemporary movement may be growing as antifa groups recruit followers on fears that fascism is making new inroads in the United States. Such expansion and the rising number of run-ins between antifa supporters and their opponents at public rallies raise the public profile of antifascism in the United States."

Congressional Research Service, *"Antifa—Background,"* 1 March 2018

Antigovernment extremists, specifically those tied to militias, racially or ethnically motivated, or "citing partisan political grievances will likely pose the greatest domestic terrorism threats in 2021."

FBI-DHS Joint Intelligence Bulletin, 2 March 2021

"The primary terrorist threat inside the United States will stem from lone offenders and small cells of individuals, including Domestic Violent Extremists (DVEs)…. Among DVEs, racially and ethnically motivated violent extremists—specifically white supremacist extremists—will remain the most persistent and lethal threat in the Homeland….Another motivating force behind domestic terrorism that also poses a threat to the Homeland is anti-government/anti-authority violent extremism.

DHS Homeland Threat Assessment, October 2020

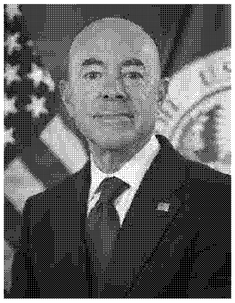
"DoD is facing a threat from domestic extremists, particularly those who espouse white supremacy or white nationalist ideologies. Some domestic extremist/terror groups (a) actively attempt to recruit military personnel into their group or cause, (b) encourage their members to join the military, or (c) join, themselves, for the purpose of acquiring combat and tactical experience. Military members are highly prized by these groups as they bring legitimacy to their causes and enhance their ability to carry out attacks."

PERSEREC, *"Leveraging FBI Resources to Enhance Military Accessions Screening and Personnel Security Vetting,"* June 2020

What DHS and FBI Say

"Domestic violent extremism poses the most lethal and persistent terrorism-related threat to our country today.... I have designated domestic violent extremism as a National Priority Area for the first time.... The Jan. 6 attack on the Capitol was one of many events that constitute a multi-year pattern of violence by domestic extremists."

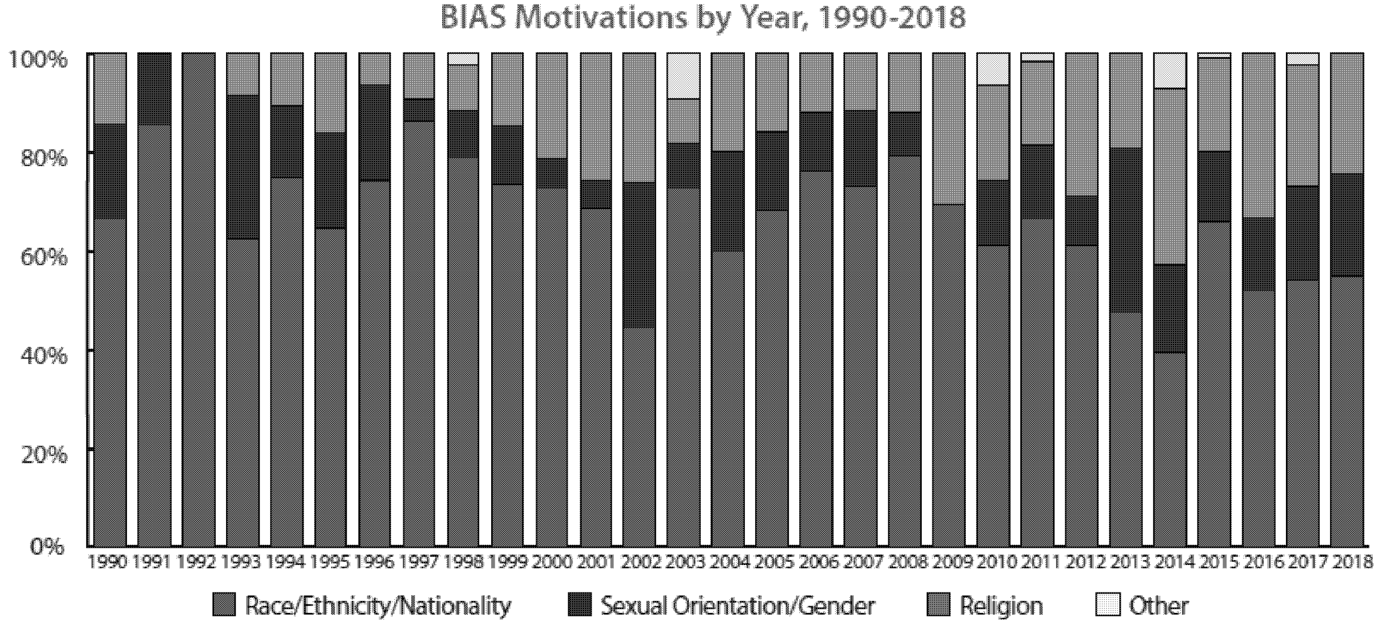
DHS Secretary Alejandro M. Mayorkis, Washington Post, "*Opinion: Alejandro Mayorkas: How my DHS will combat domestic extremism,*" 25 February 2021



"That attack [6 January 2021 attack on the US Capitol], that siege, was criminal behavior. It is behavior that we, the FBI, view as domestic terrorism....The problem of domestic terrorism has been metastasizing across the country for a long time now and it's not going away anytime soon."

FBI Director Christopher Wray Congressional testimony, 2 March 2021

Motivations and Characteristics of Hate Crime Offenders



"Bias towards individuals on the basis of race, ethnicity, or nationality is the most prevalent category….Offenders motivated by bias on religion and sexual orientation are the second and third most common motivations….From 2013-2018, the data show an increase in the number of offenders with these motivations."

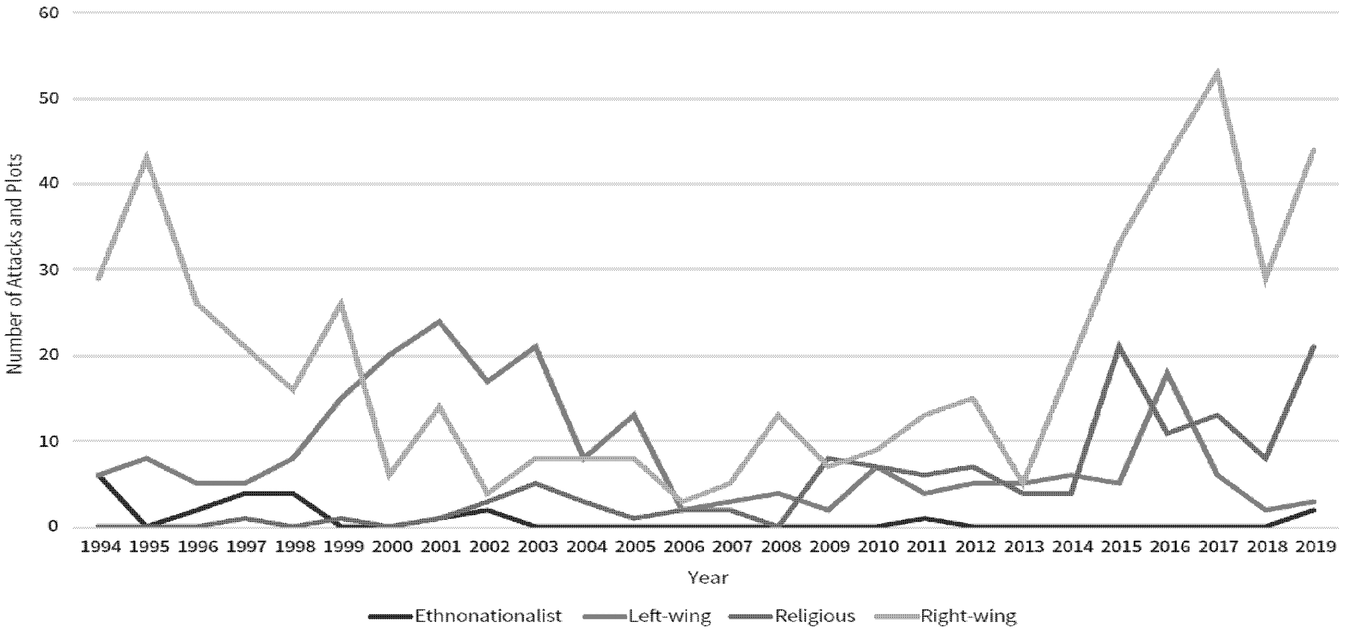
START/University of Maryland, *"Motivations and Characteristics of Hate Crime Offenders,"* October 2020

The Escalating Terrorism Problem in the United States

Center for Strategic and International Studies (CSIS)

June 2020

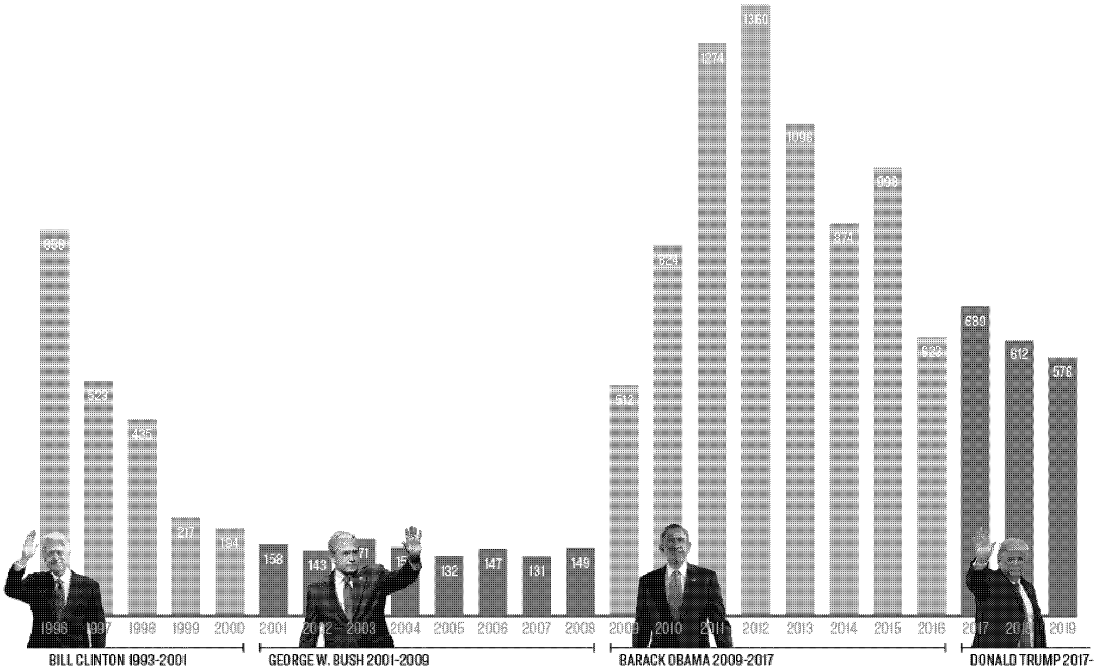
Figure 2: Number of Terrorist Attacks and Plots by Perpetrator Orientation, 1994-2019



"Between 1994 and 2020, there were 893 terrorist attacks and plots in the United States. Overall, right-wing terrorists perpetrated the majority—57 percent—of all attacks and plots during this period, compared to 25 percent committed by left-wing terrorists, 15 percent by religious terrorists, 3 percent by ethnonationalists, and 0.7 percent by terrorists with other motives."

Anti-Government Groups

ANTIGOVERNMENT 'PATRIOT' GROUPS 1995–2019



Southern Poverty Law Center
https://www.splcenter.org/fighting-hate/extremist-files/ideology/antigovernment

QAnon

- As of 24 February 2021, 56 QAnon followers have committed ideologically-motivated crimes in the US—including 27 who have participated in the 6 January 2021 attack on the US Capitol

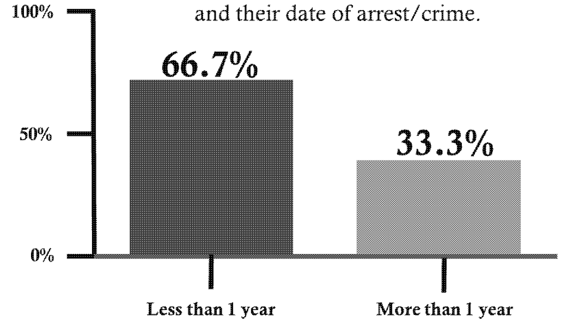
- Women were 19% of non-Capitol offenders and 24% of Capitol rioters

- Sixty-eight (68%) percent of non-Capitol offenders have documented mental health concerns—these include post-traumatic stress disorder, paranoid schizophrenia, bipolar disorder, and Munchausen syndrome by proxy—according to court records and other public sources

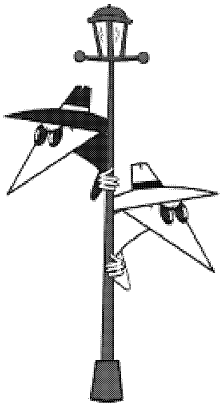
- Forty-four (44%) percent on non-Capitol offenders radicalized after experiencing a traumatic event—premature deaths of loved ones; physical, emotional, or sexual abuse; post-traumatic stress disorder from military service
  - 83% of women non-Capitol offenders experienced trauma which involved physical and/or sexual abuse of their children by a romantic partner or family member

- While some extremists radicalize over extended periods of time, data indicates the majority radicalized in less than a year, and some in mere weeks

From Radicalization to Mobilization – Measured as period of time between evidence of an individual's first exposure to extremist views and their date of arrest/crime.

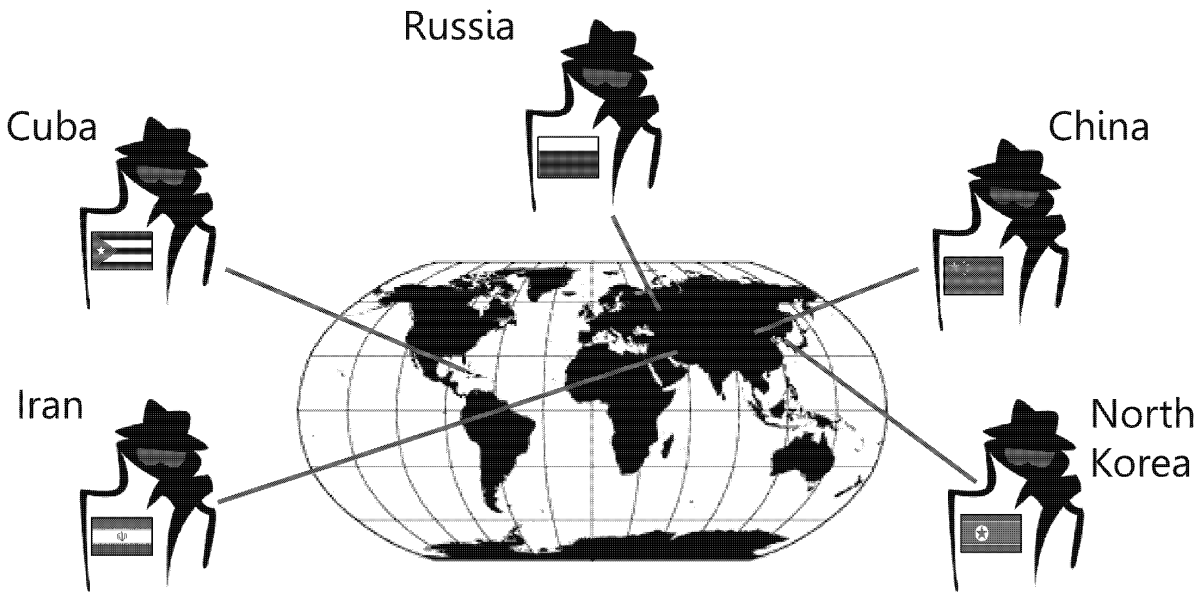


START/University of Maryland, *"QAnon Offenders in the United States,"* February 2021



ESPIONAGE

Espionage – Nation State Threats



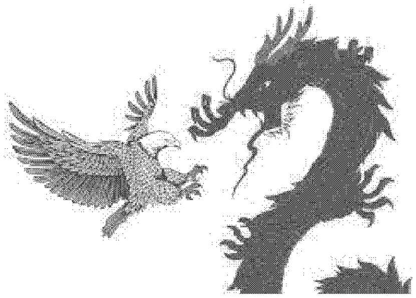
President Joseph R. Biden, *"Interim National Security Strategic Guidance,"* March 2021

Daniel R. Coats, *"Senate Select Committee on Intelligence Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community,"* ODNI, 29 January 2019

Growing Chinese Intelligence Threat

“About 80 percent of all economic espionage prosecutions brought by the US Department of Justice (DOJ) allege conduct that would benefit the Chinese state, and there is at least some nexus to China in around 60 percent of all trade secret theft cases.”

DOJ, *“Information About the DOJ’s China Initiative and a Compilation of China-Related Prosecutions Since 2018,”* Updated 5 May 2021



Espionage/Espionage-related arrests have doubled every 10 years

2010-2020 – 14
2000-2009 – 6
Pre-2000 – 3

Exploiting social networking sites for spotting, initial contact, and developing relationships

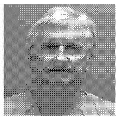
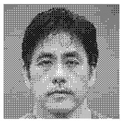
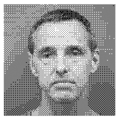
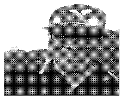
Targets are multi-gender/multi-ethnic

Money/financial gain a primary motivation/driver

Personal meetings in China

Extensive cyber operations

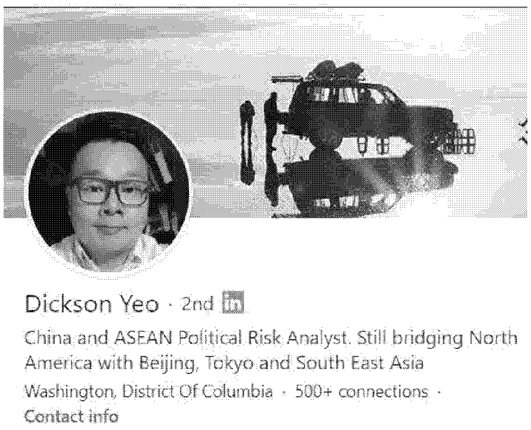
Recently Arrested Chinese Spies

Name	Years Spying	Spotted	Meetings	Motivation
Candace Claiborne USDS	2011 - 2017	China	China	Financial Blackmail
 Ron Rockwell Hansen DIA (former)	2014 - 2018	China – Printed Out LinkedIn Profiles on Colleagues for MSS	China	Financial Thrill Seeking Ego
 Jerry Chun Lee CIA (former)	2010 - 2013	China	China	Financial
 Kevin Mallory CIA/DIA (former)	2017 - 2018	LinkedIn	China	Financial
 Alexander Ma CIA (former) FBI	At least 2001 – 2010	China	China	Financial

Tell Me Your Woes

Dickson Yeo, aka, Jun Wei – Singaporean plead guilty in July 2020 for actively recruiting sources for Chinese intelligence

- Used LinkedIn to target and build contacts by using fake consulting firm (tasked by Chinese in 2018 to do so)
- "Received over 400 resumes…90% were from US Government personnel with security clearances" and he would pass more interesting ones to his Chinese intelligence officers
- Chinese handlers trained Yeo on how to elicit information from his potential targets and identify those who were "dissatisfied with work, were having financial troubles, had child support" and develop good rapport
- Relocated to WDC from January-July 2019



Dickson Yeo · 2nd in

China and ASEAN Political Risk Analyst. Still bridging North America with Beijing, Tokyo and South East Asia

Washington, District Of Columbia · 500+ connections ·

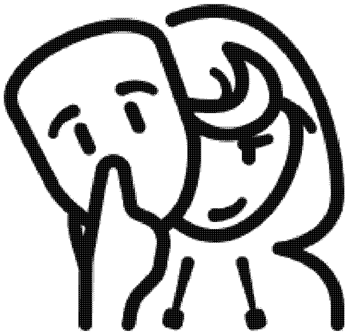
Contact info

Three US citizen examples

- Worker on USAF F-35B with high level national security clearance – told Yeo he ***was having financial difficulties.***
- US Army officer stationed at Pentagon – told Yeo he ***was traumatized by his multiple tours in Afghanistan.*** In November 2019 tasked to turn the officer into a "permanent conduit of information."
- USDS employee – confided to Yeo he was ***dissatisfied at work and had financial difficulties***

China Not Only Country Exploiting LinkedIn – Nor Exploiting for Advantage Against the United States

"*At least 10,000 UK nationals have been approached by fake profiles linked to hostile states*…[on] LinkedIn, over the past five years, according to MI5…. "Malicious profiles" are being used on "an industrial scale," the security agency's chief, Ken McCallum, said."



BBC, *"MI5 Warns of Spies Using LinkedIn to Trick Staff Into Spilling Secrets,"* 20 April 2021

"As far back as 2015, the cybersecurity company Secureworks reported that an Iran-based threat group it called TG-2889 was operating a network of fake LinkedIn profiles."

CNBC, *"Here's Why LinkedIn Is a 'Gold Mine" for Foreign Spies Digging for Corporate and Government Secrets,"* 8 November 2019

"***LinkedIn provides a rich hunting ground for Russian agents***…. 'The Russian special services are for sure exploiting LinkedIn to gather personal information on certain targets and possibly recruit and blackmail them," says a close Kremlin watcher at a university in a former Soviet satellite state…' They operate under fabricated identities and credentials."

Newsweek, *"How Russia is Using LinkedIn as a Tool of War Against its US Enemies,"* 8 August 2017

"***China is using fake LinkedIn profiles to gather information on German officials and politicians, the German intelligence agency (BfV) has said.*** The agency alleges that Chinese intelligence used the networking site to target at least 10,000 Germans, possibly to recruit them as informants. It released a number of fake profiles allegedly used for this purpose."

BBC, *"German Spy Agency Warns of Chinese LinkedIn Espionage,"* 10 December 2017

Date	Major Chinese Government Breaches
???? - December 2020	Suspected Chinese hackers exploited a flaw in software made by SolarWinds Corp to help break into U.S. government computers—the **National Finance Center (NFC)**, a federal payroll agency inside the **US Department of Agriculture**, was among the affected organizations. The NFC is responsible for handling the payroll of more than 160 government agencies and includes federal employee social security numbers, phone numbers and personal email addresses as well as banking information.
April 2020	US officials reported seeing a surge of attacks by Chinese hackers against healthcare providers, pharmaceutical manufacturers, and the **US Department of Health and Human Services** amidst the COVID-19 pandemic.
December 2018	Hundreds of gigabytes of data stolen from computers of more than 45 technology companies and US Government agencies. Also stole names, SSNs, DOBs, salary info, phone numbers, and email addresses of more than 100,000 **US Navy** personnel.
September 2018	Since 2014, Starwood hotel chain network breach with estimated personal information of up to 500 million people stolen. Exposed an unusually broad array of data including names, addresses, phone numbers, passport numbers, and credit card numbers, as well as information on where people traveled and with whom.
March 2017	PII of hundreds of millions of people (potentially 143 million) stolen from Equifax, one of the credit reporting agencies that assess the financial health of nearly everyone in the United States.
May 2015	Significant amounts of customer data stolen from United Airlines.
February 2015	Anthem/Blue Cross Blue Shield hack compromised the sensitive personal information of approximately 78.8 million Americans.
April 2015	**OPM** discovered its networks infiltrated and personal information of federal employees, including security clearance information, stolen.
November 2014	**US Postal Service** computer networks breached and data of approximately 800,000 employees exfiltrated.
August 2014	**US Investigations Services** network infiltrated. One of the first steps in the 2015 OPM hack. Community Health Systems disclosed its networks infiltrated and personal information from 4.5 million patients stolen.

You Make the Call – What Are the Indicators?

Former State Department Employee Indicted for Concealing Information in Background Investigation

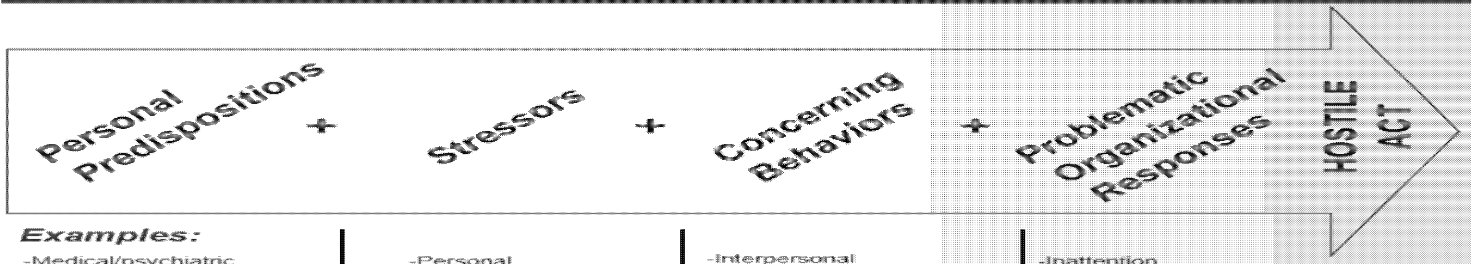
WASHINGTON – Paul Michael Guertin ("Guertin"), 40, of Arizona and former resident of Washington, DC, was indicted on March 29, 2021 by a federal grand jury in the District of Columbia for wire fraud and obstructing an official proceeding. The indictment was announced by Acting U.S. Attorney Channing D. Phillips and Special Agent in Charge Elisabeth Heller, of the U.S. Department of State, Office of Inspector General.

Guertin was a Foreign Service Officer who served on multiple State Department assignments, including overseas postings to U.S. diplomatic missions in Shanghai, China and Islamabad, Pakistan, and a posting to the Bureau of Intelligence and Research at State Department headquarters in Washington, DC. As a condition of his employment, Guertin was required to apply for and maintain a Top Secret security clearance. According to the indictment, Guertin intentionally concealed information on his SF-86 background investigation questionnaires and in interviews with State Department background investigators. He withheld information about several categories of conduct, including an undisclosed sexual relationship with a Chinese national whose U.S. visa application was adjudicated by Guertin while he was serving as a consular officer in Shanghai, China; undisclosed gambling debts, and an undisclosed $225,000 loan from two Chinese nationals, who were directed by Guertin to provide $45,000 of the initial disbursement in the form of cash in $100 bills.

https://www.justice.gov/usao-dc/pr/former-state-department-employee-indicted-concealing-information-background-investigation

Shaw's Critical Path - Guertin

Factors Along the Critical Path to Insider Risk



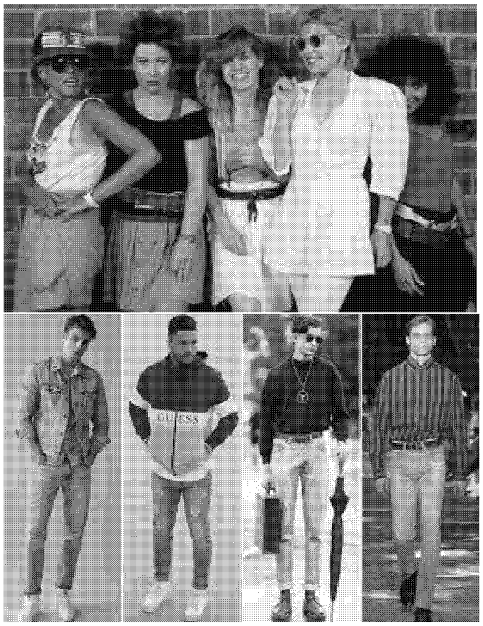
Examples:

Personal Predispositions	Stressors	Concerning Behaviors	Problematic Organizational Responses
-Medical/psychiatric conditions -Personality or social skills issues -Previous rule violations -Social network risks	-Personal -Professional -Financial	-Interpersonal -Technical -Security -Financial -Personnel -Mental health/addictions -Social network -Travel	-Inattention -No risk assessment process -Inadequate investigation -Summary dismissal or other actions that escalate risks
Undisclosed sexual relationship with Chinese national – sexual addiction? Personality or social skills issues? Undisclosed gambling debts – gambling addiction?	Undisclosed gambling debts – financial? Undisclosed $225,000 loan from two Chinese nationals – financial?	Intentionally concealing information on SF-86 and USDS background interviewers Undisclosed sexual relationship with Chinese national Undisclosed $225,000 loan from two Chinese nationals – financial? Provide initial $45,000 of loan in cash ($100 bills)	

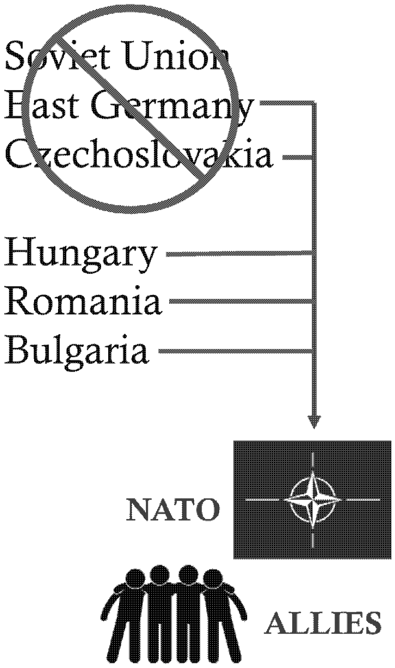
Do Nation State Threats Stay the Same?

Let's go back in time….

say….1985



Who were the big threats?



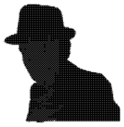
~~Soviet Union~~
~~East Germany~~
~~Czechoslovakia~~

Hungary
Romania
Bulgaria

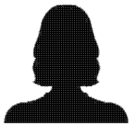
NATO

ALLIES

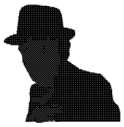
Are Nation States the Only Concern?



Aws Muwafaq Abduljabber
Living in Jordan since 2010 and led efforts



Olesya Leonidovna Krasilova
Employed by US Citizenship and Immigration Service (Aug 2011 – Feb 2019);
Worked in US Embassy in Moscow, Russia



Haithan Isa Saado Sad
Employed by US Citizenship and Immigration Service (Nov 2007 – Jan 2016);
Worked in US Embassy in Amman, Jordan

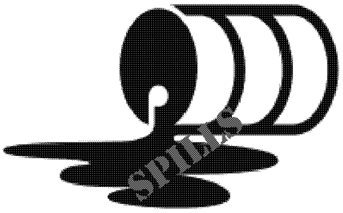
Two former US State Department employees indicted in January 2021 stealing information related to the US Refugee Admissions Program (USRAP) and, in particular, the Iraq P-2 program, which allows certain Iraqis to apply directly for refugee resettlement in the United States.

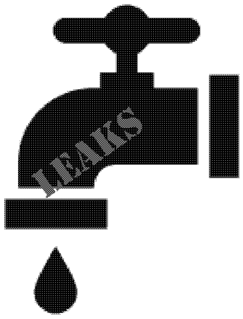
From approximately February 2016 until at least April 2019, the two stole and sold USRAP information to a Jordanian-based individual, who would use it to assist applicants in gaining admission to the United States through fraudulent means. The records contained sensitive, non-public information about refugee applicants, their family members, their employment and military history, their accounts of persecution or fear of persecution, the results of security checks, and internal assessments by US officials regarding applications.

The theft of USRAP records creates a number of risks to public safety and national security while imposing significant costs on the US Government, its taxpayers, and otherwise legitimate refugee applicants negatively impacted by the scheme.

Department of Justice, *"Former U.S. Government Employee Pleads Guilty To Conspiracy To Steal U.S. Government Records and Defraud U.S. Refugee Program,"* 26 January 2021

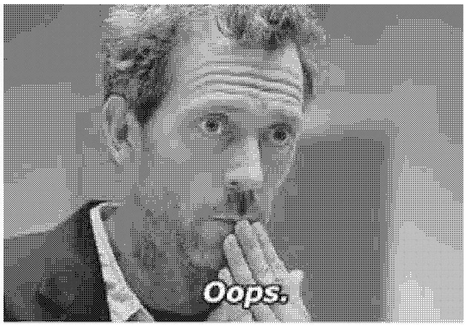
UNAUTHORIZED DISCLOSURE





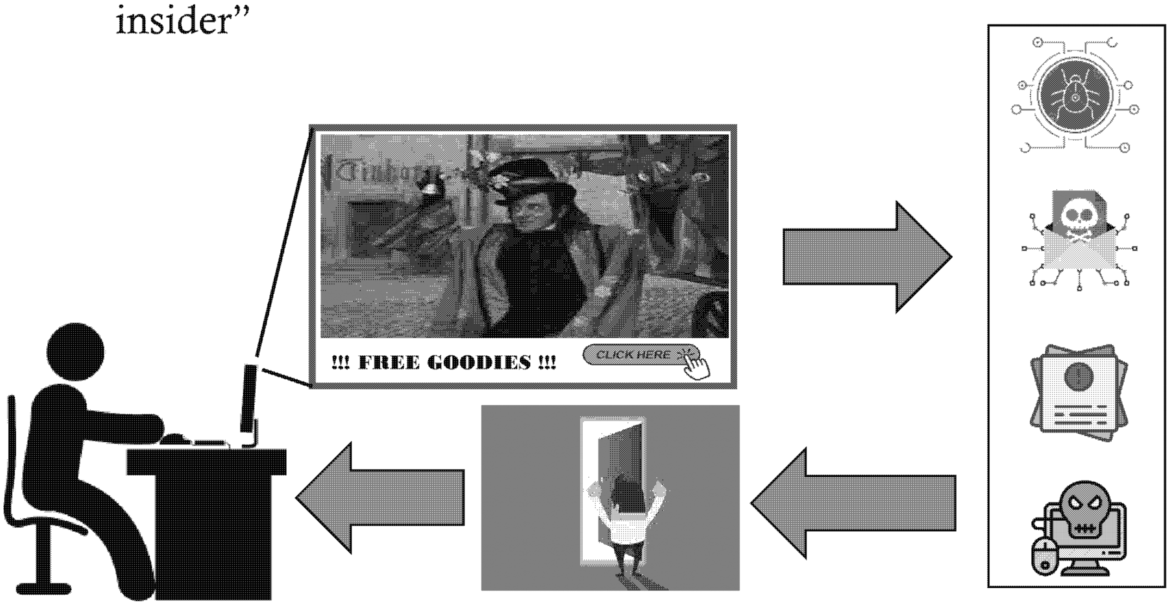
Unauthorized Disclosure – Spills

Negligent, **inadvertent disclosures** of classified information or Controlled Unclassified Information (CUI) transferred onto an information system **not authorized** at the appropriate security level or not having the required CUI protection or access controls.



Unauthorized Disclosure – Spacks and Brills

“Hostile actors gaining access to target information or resources—computer networks—usually through inadvertent or careless online activities by an insider”

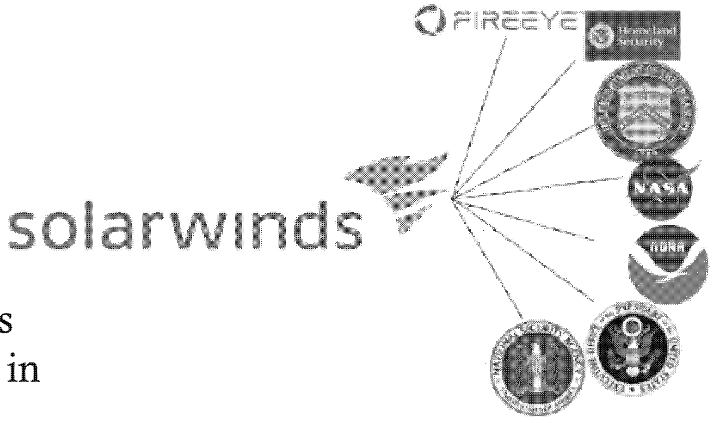


Downloading malware through opening email attachments—such as pdfs—or accessing compromised websites

Unauthorized Disclosure – Spacks and Brills

New challenge – **<u>automated attacks without role of any insider</u>**

- IT management products which provide automation of certain activities such as deploying updates



SolarWinds attack – December 2020 FireEye reported a malicious actor was exploiting a supply chain vulnerability in SolarWinds products to hack into US Government and private sector IT networks

https://crsreports.congress.gov/product/pdf/IN/IN11559

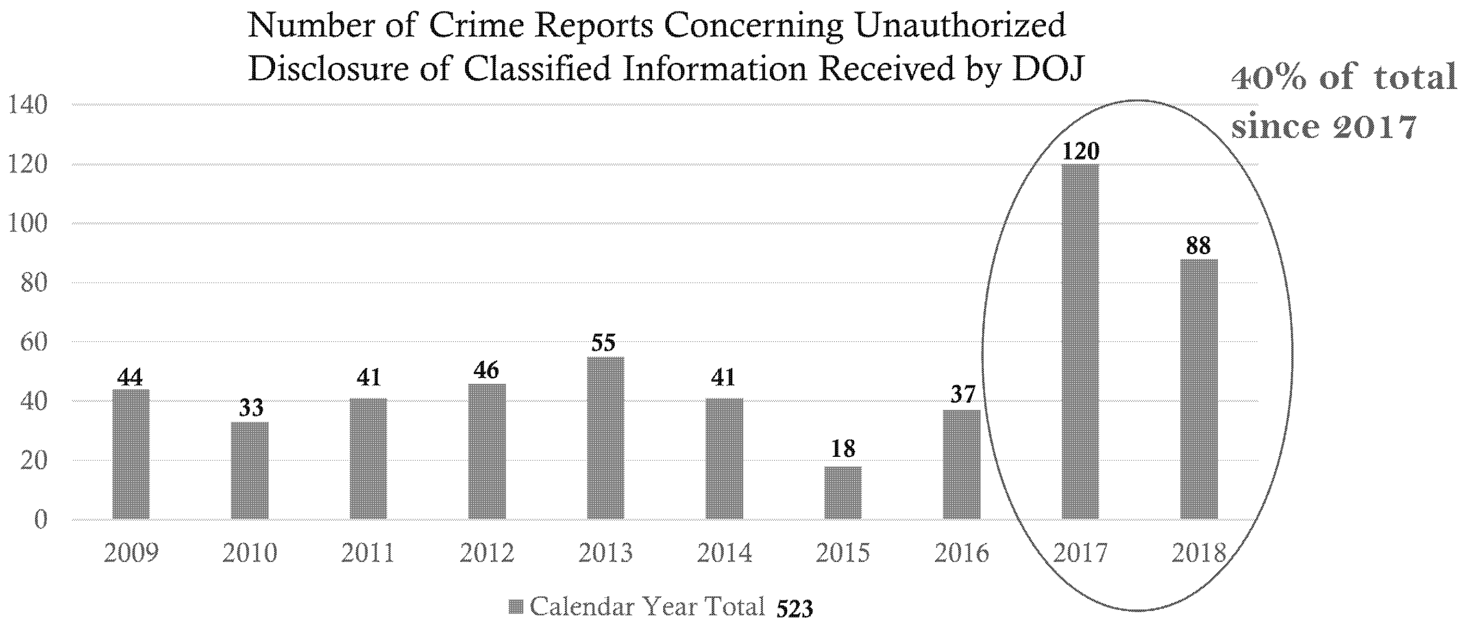
Unauthorized Disclosure - Leaks

- More workers have access to more information – opportunity and vulnerability increases
- Non-state actors pose significant threat – threat actor involvement
- Motivations – non-monetary/ financial (disgruntlement, ideology, ego, thrill-seeking)

Frank and Ernest by Thaves May 27, 2021

VEGETABLE INTELLIGENCE AGENCY
PEOPLE, I'M AFRAID THERE'S A LEEK IN OUR ORGANIZATION!
5-27 THAVES
©2021 Thaves/Dist. by Andrews McMeel Synd.

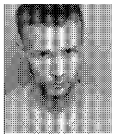
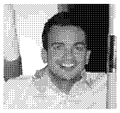
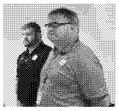
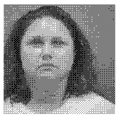
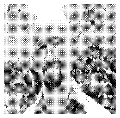
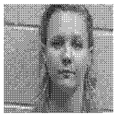
Unauthorized Disclosure – Investigations



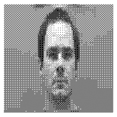
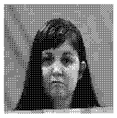
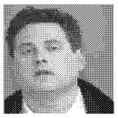
40% of total since 2017

https://fas.org/irp/agency/doj/crimes-reports-2016.html
https://fas.org/irp/agency/doj/crimes-reports.html
https://fas.org/irp/agency/doj/crimes-reports-2017-18.pdf

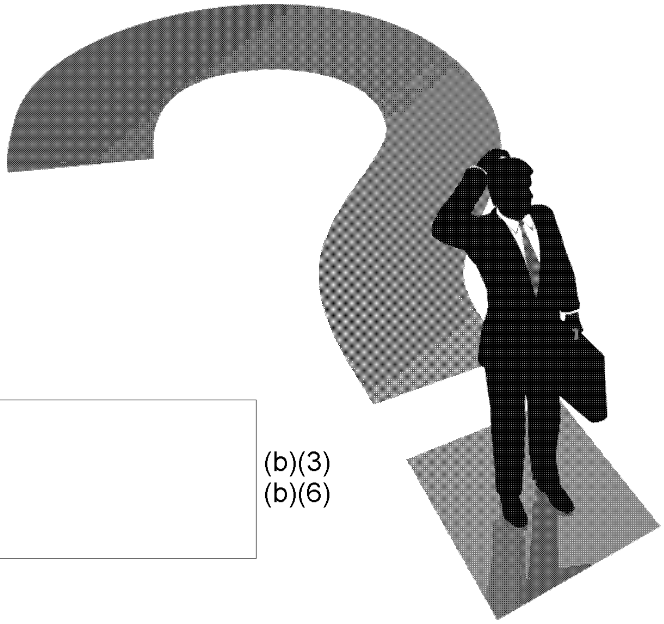
Recent Unauthorized Disclosure (Leaks) Arrests

Name	Year of Activity	Provided To	Motivation
 Daniel Everette Hale NGA (contractor)	2013 - 2014	The Intercept	Political? Personal?
 Henry Kyle Freese DIA	2019	NBC, CNBC	Personal Relationship
 John Fry IRS	2018	Michael Avennati, The New Yorker	Political
 Natalie Sours Edwards Department of Treasury	2017 - 2018	BuzzFeed	Political
 Joshua Schulte CIA (contractor)	2017	WikiLeaks	Political Disgruntlement
 Reality Winner NSA (contractor)	2017	The Intercept	Political

Other Unauthorized Disclosure Arrests

Name	Year of Activity	Provided To	Motivation
Kendra Kingsbury FBI	2004 - 2017	???	???
 Itzaak Vincent Kemp AFRL/NASIC (contractor)	2016 - 2019	???	???
 Elizabeth Jo Shirley NSA, ONI, DOE, DOD, NCIJTF, DOD contractors	1994 - 2002	???	Planned to offer to Russian Government officials in Mexico for help to resettle her and her daughter in Russia
 Harold Thomas Martin NSA (contractor)	~2014 - 2016	???	???

Questions?



[redacted] (b)(3)
(b)(6)

DEPARTMENT OF JUSTICE

Insider Threat Trends

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Updated: 26 Apr 2021

Objectives

1. Discuss current trends in Espionage
2. Discuss current trends in Unauthorized Disclosure
3. Discuss current trends in Workplace Violence
4. Discuss current trends in Domestic Violent Extremism

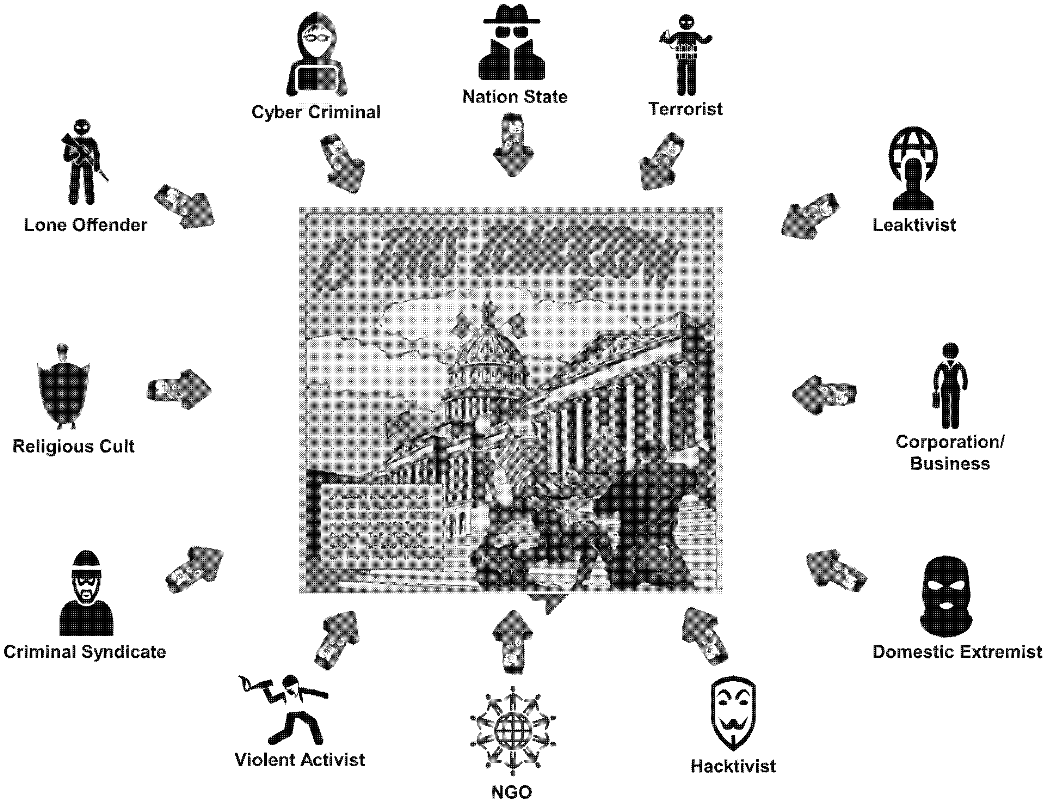
Key Assumptions

1. Population of US Federal Government/US Military personnel mirror US population

2. Major insider threat event is a rare occurrence – based on low number of reported incidents over the years

3. Risk of a major insider threat event is growing – based on larger number of threat actors, and increased opportunity and vulnerabilities compared to past years

Threat Actors – Who Are They?


IS THIS TOMORROW
IT WASN'T LONG AFTER THE END OF THE SECOND WORLD WAR THAT COMMUNIST FORCES IN AMERICA SEIZED THEIR CHANCE. THE STORY IS SAD... THE END TRAGIC... BUT THIS IS THE WAY IT BEGAN...

Cyber Criminal

Nation State

Terrorist

Lone Offender

Leaktivist

Religious Cult

Corporation/ Business

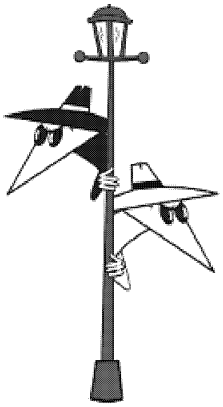
Criminal Syndicate

Domestic Extremist

Violent Activist

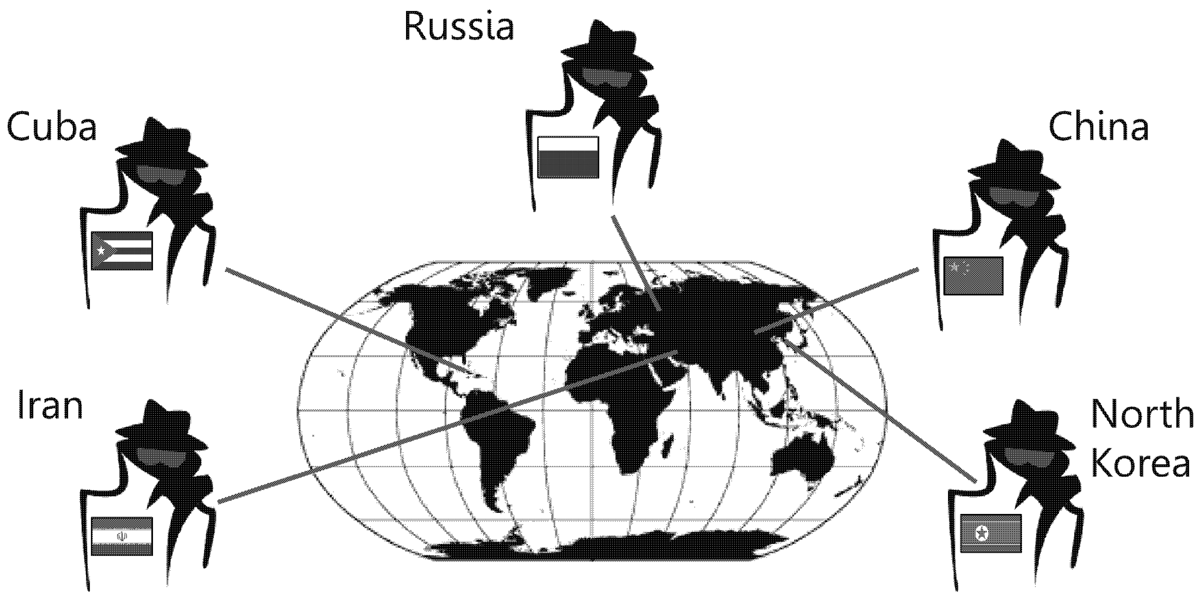
NGO

Hacktivist



ESPIONAGE

Espionage – Nation State Threats



President Joseph R. Biden, *"Interim National Security Strategic Guidance,"* March 2021

Daniel R. Coats, *"Senate Select Committee on Intelligence Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community,"* ODNI, 29 January 2019

Growing Chinese Intelligence Threat

Espionage/Espionage-related arrests have doubled every 10 years

2010-2020 – 14
2000-2009 – 6
Pre-2000 – 3

Exploiting social networking sites for spotting, initial contact, and developing relationships

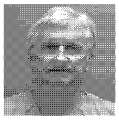
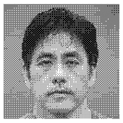
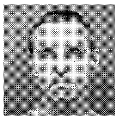
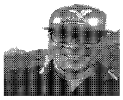
Targets are multi-gender/multi-ethnic

Money/financial gain a primary motivation/driver

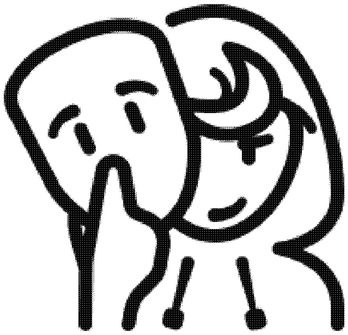
Personal meetings in China

Extensive cyber operations

Recently Arrested Chinese Spies

Name	Years Spying	Spotted	Meetings	Motivation
Candace Claiborne USDS	2011 - 2017	China	China	Financial Blackmail
 Ron Rockwell Hansen DIA (former)	2014 - 2018	China – Printed Out LinkedIn Profiles on Colleagues for MSS	China	Financial Thrill Seeking Ego
 Jerry Chun Lee CIA (former)	2010 - 2013	China	China	Financial
 Kevin Mallory CIA/DIA (former)	2017 - 2018	LinkedIn	China	Financial
 Alexander Ma CIA (former) FBI	At least 2001 – 2010	China	China	Financial

China Not Only Country Exploiting LinkedIn



*"**At least 10,000 UK nationals have been approached by fake profiles linked to hostile states**...[on]* LinkedIn, over the past five years, according to MI5.... "Malicious profiles" are being used on "an industrial scale," the security agency's chief, Ken McCallum, said."

BBC, *"MI5 Warns of Spies Using LinkedIn to Trick Staff Into Spilling Secrets,"* 20 April 2021

"As far back as 2015, the cybersecurity company Secureworks reported that an Iran-based threat group it called TG-2889 was operating a network of fake LinkedIn profiles."

CNBC, *"Here's Why LinkedIn Is a 'Gold Mine" for Foreign Spies Digging for Corporate and Government Secrets,"* 8 November 2019

"***LinkedIn provides a rich hunting ground for Russian agents***.... 'The Russian special services are for sure exploiting LinkedIn to gather personal information on certain targets and possibly recruit and blackmail them," says a close Kremlin watcher at a university in a former Soviet satellite state...' They operate under fabricated identities and credentials."

Newsweek, *"How Russia is Using LinkedIn as a Tool of War Against its US Enemies,"* 8 August 2017

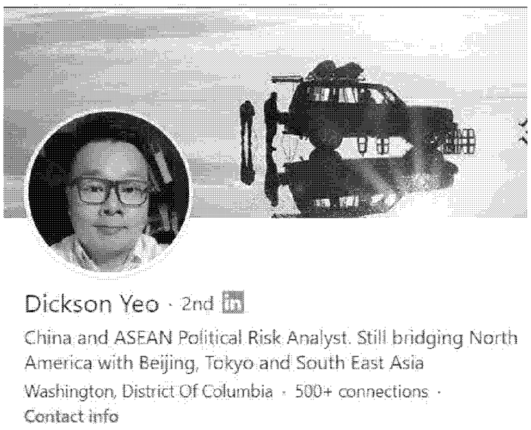
"China is using fake LinkedIn profiles to gather information on German officials and politicians, the German intelligence agency (BfV) has said. The agency alleges that Chinese intelligence used the networking site to target at least 10,000 Germans, possibly to recruit them as informants. It released a number of fake profiles allegedly used for this purpose."

BBC, *"German Spy Agency Warns of Chinese LinkedIn Espionage,"* 10 December 2017

Tell Me Your Woes

Dickson Yeo, aka, Jun Wei – Singaporean plead guilty in July 2020 for actively recruiting sources for Chinese intelligence

- Used LinkedIn to target and build contacts by using fake consulting firm (tasked by Chinese in 2018 to do so)
- "Received over 400 resumes…90% were from US Government personnel with security clearances" and he would pass more interesting ones to his Chinese intelligence officers
- Chinese handlers trained Yeo on how to elicit information from his potential targets and identify those who were "dissatisfied with work, were having financial troubles, had child support" and develop good rapport
- Relocated to WDC from January-July 2019



Dickson Yeo · 2nd in

China and ASEAN Political Risk Analyst. Still bridging North America with Beijing, Tokyo and South East Asia

Washington, District Of Columbia · 500+ connections · Contact info

Three US citizen examples

- Worker on USAF F-35B with high level national security clearance – told Yeo he ***was having financial difficulties.***
- US Army officer stationed at Pentagon – told Yeo he ***was traumatized by his multiple tours in Afghanistan.*** In November 2019 tasked to turn the officer into a "permanent conduit of information."
- USDS employee – confided to Yeo he was ***dissatisfied at work and had financial difficulties***

You Make the Call – What Are the Indicators?

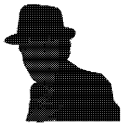
Former State Department Employee Indicted for Concealing Information in Background Investigation

WASHINGTON – Paul Michael Guertin ("Guertin"), 40, of Arizona and former resident of Washington, DC, was indicted on March 29, 2021 by a federal grand jury in the District of Columbia for wire fraud and obstructing an official proceeding. The indictment was announced by Acting U.S. Attorney Channing D. Phillips and Special Agent in Charge Elisabeth Heller, of the U.S. Department of State, Office of Inspector General.

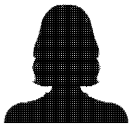
Guertin was a Foreign Service Officer who served on multiple State Department assignments, including overseas postings to U.S. diplomatic missions in Shanghai, China and Islamabad, Pakistan, and a posting to the Bureau of Intelligence and Research at State Department headquarters in Washington, DC. As a condition of his employment, Guertin was required to apply for and maintain a Top Secret security clearance. According to the indictment, Guertin intentionally concealed information on his SF-86 background investigation questionnaires and in interviews with State Department background investigators. He withheld information about several categories of conduct, including an undisclosed sexual relationship with a Chinese national whose U.S. visa application was adjudicated by Guertin while he was serving as a consular officer in Shanghai, China; undisclosed gambling debts and an undisclosed $225,000 loan from two Chinese nationals who were directed by Guertin to provide $45,000 of the initial disbursement in the form of cash in $100 bills.

https://www.justice.gov/usao-dc/pr/former-state-department-employee-indicted-concealing-information-background-investigation

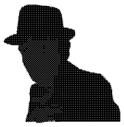
Non-Nation State Activity: Criminal Motivation



Aws Muwafaq Abduljabber
Living in Jordan since 2010 and led efforts



Olesya Leonidovna Krasilova
Employed by US Citizenship and Immigration Service (Aug 2011 – Feb 2019);
Worked in US Embassy in Moscow, Russia



Haithan Isa Saado Sad
Employed by US Citizenship and Immigration Service (Nov 2007 – Jan 2016);
Worked in US Embassy in Amman, Jordan

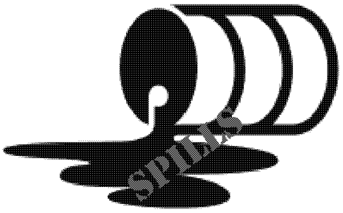
Two former US State Department employees indicted in January 2021 stealing information related to the US Refugee Admissions Program (USRAP) and, in particular, the Iraq P-2 program, which allows certain Iraqis to apply directly for refugee resettlement in the United States.

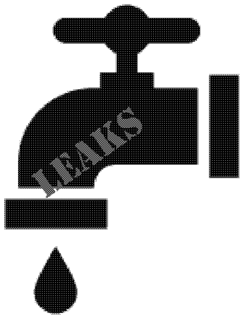
From approximately February 2016 until at least April 2019, the two stole and sold USRAP information to a Jordanian-based individual, who would use it to assist applicants in gaining admission to the United States through fraudulent means. The records contained sensitive, non-public information about refugee applicants, their family members, their employment and military history, their accounts of persecution or fear of persecution, the results of security checks, and internal assessments by US officials regarding applications.

The theft of USRAP records creates a number of risks to public safety and national security while imposing significant costs on the US Government, its taxpayers, and otherwise legitimate refugee applicants negatively impacted by the scheme.

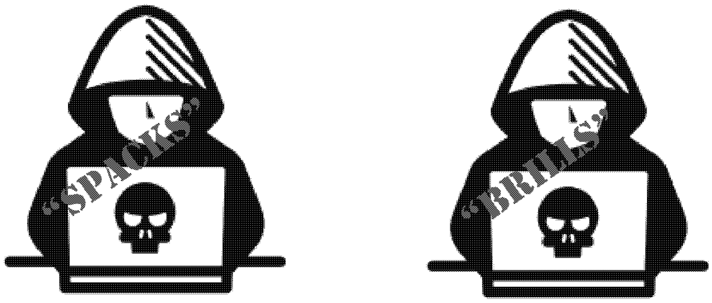
Department of Justice, *"Former U.S. Government Employee Pleads Guilty To Conspiracy To Steal U.S. Government Records and Defraud U.S. Refugee Program,"* 26 January 2021

UNAUTHORIZED





DISCLOSURE

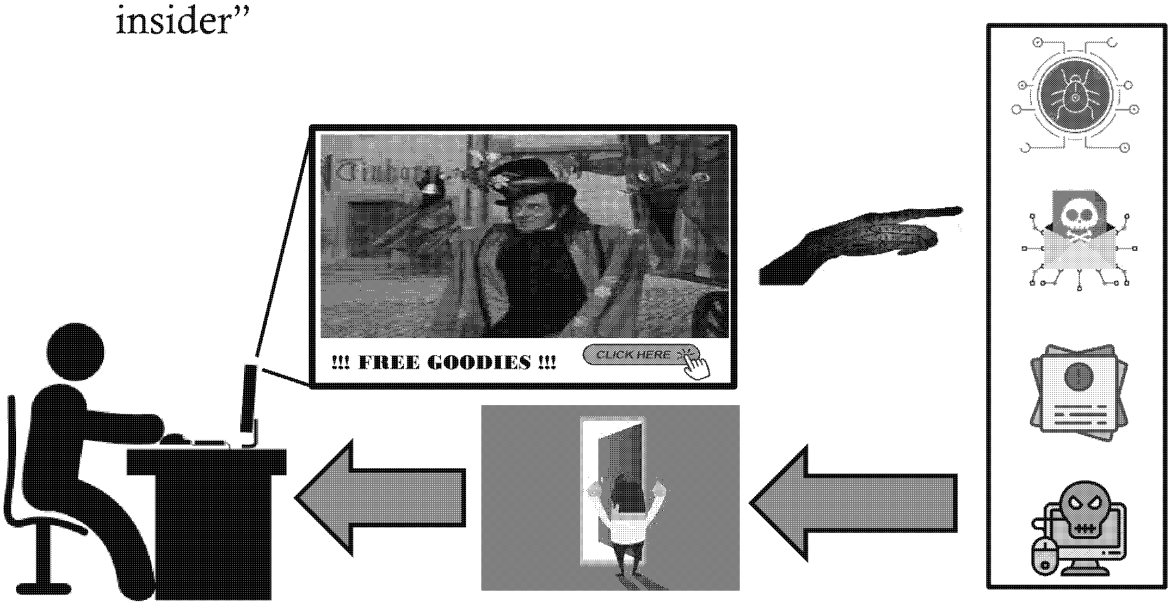


Unauthorized Disclosure – Spills

Negligent, **inadvertent disclosures** of classified information or Controlled Unclassified Information (CUI) transferred onto an information system **not authorized** at the appropriate security level or not having the required CUI protection or access controls.

Unauthorized Disclosure – Spacks and Brills

“Hostile actors gaining access to target information or resources—computer networks—usually through inadvertent or careless online activities by an insider”



Downloading malware through opening email attachments—such as pdfs—or accessing compromised websites

Cyber Criminals – Biggest Threat?

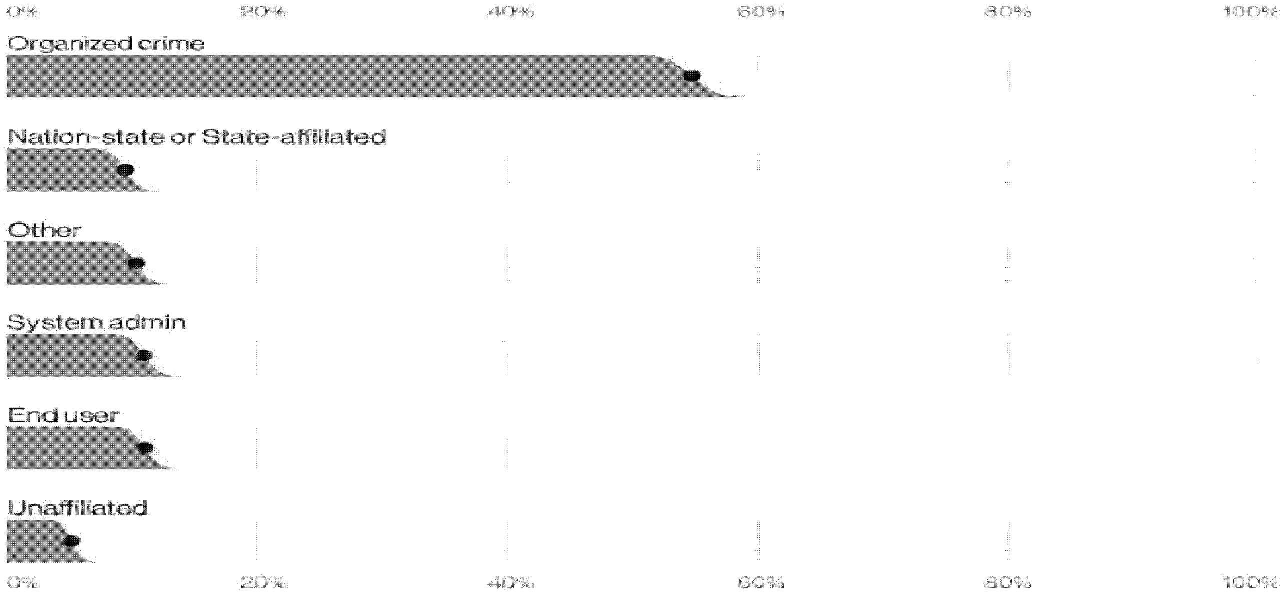


Figure 10. Top Actor varieties in breaches (n = 977)

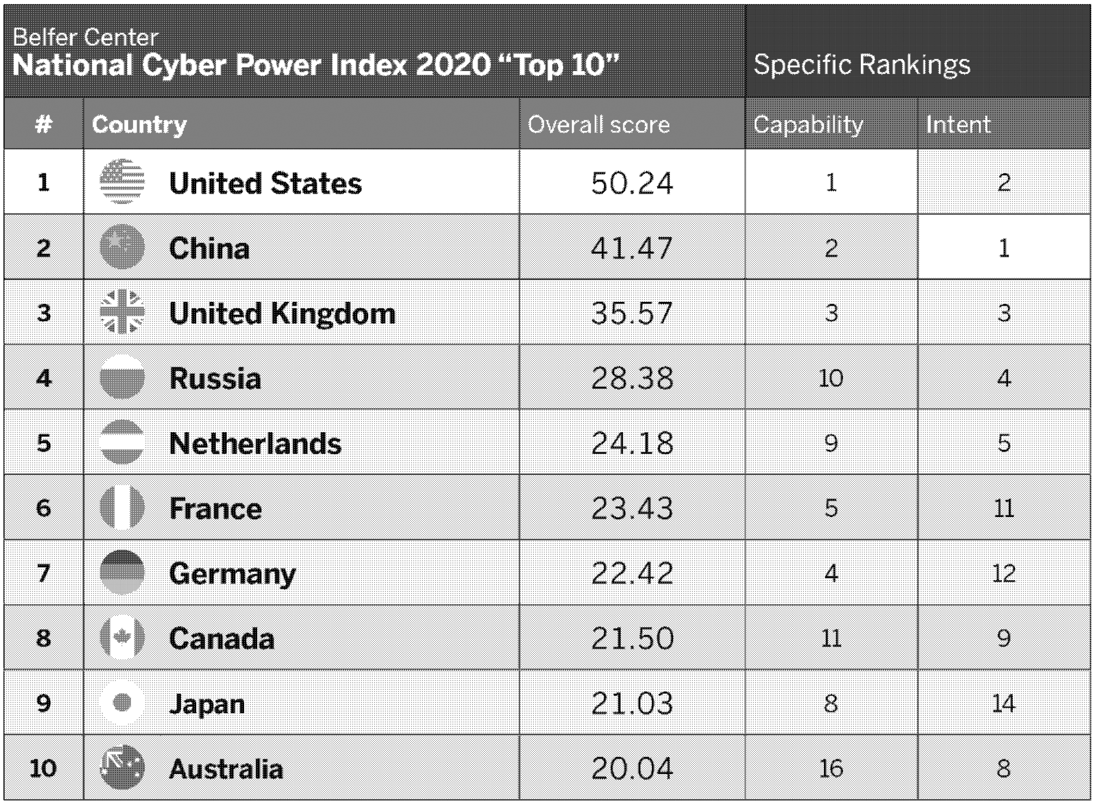
Verizon 2020 Data Breach Investigations Report

Cyber Threat Matrix

	Profit/ Financial Gain	Collection & Surveillance	Offensive Attack
Established Actors (AEs) – Those with most advanced, accurate, and agile tools. Have extensive resources—including time and money—to achieve persistence and capable of achieving global reach using advanced tradecraft.		Nation State	Nation State
Emerging Actors – Have defined processes, capabilities, and a history of targeted operations/activities but are not consistently successful to the extent of AEs. Tradecraft is limited, have beginning of organizational maturity, and are on cusp of developing products, processes, and people necessary to be AEs.	Cyber Criminal Nation State Terrorist	Nation State Terrorist	Nation State Terrorist
Opportunistic Actors – Generally associated with low-level cyber criminal activities. Market they operate in are dispersed, diverse, and segregated for tools to acquire. Are consistently innovating to keep pace with current trends and avoid law enforcement intervention.	Cyber Criminal → Can Include → Terrorist Domestic Extremist Hacktivist Violent Activist Lone Offender Religious Cult Nation State*		

Public/Private Analytic Exchange/DHS, *"Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar,"* 2019

Nation State Cyber Threat Rankings



Belfer Center
National Cyber Power Index 2020 "Top 10"

#	Country	Overall score	Specific Rankings Capability	Intent
1	United States	50.24	1	2
2	China	41.47	2	1
3	United Kingdom	35.57	3	3
4	Russia	28.38	10	4
5	Netherlands	24.18	9	5
6	France	23.43	5	11
7	Germany	22.42	4	12
8	Canada	21.50	11	9
9	Japan	21.03	8	14
10	Australia	20.04	16	8

Belfer Center for Science and International Affairs/Harvard Kennedy School, *"National Cyber Power Index 2020,"* September 2020

Date	Major Chinese Government Breaches
???? - December 2020	Suspected Chinese hackers exploited a flaw in software made by SolarWinds Corp to help break into U.S. government computers—the **National Finance Center (NFC)**, a federal payroll agency inside the **US Department of Agriculture**, was among the affected organizations. The NFC is responsible for handling the payroll of more than 160 government agencies and includes federal employee social security numbers, phone numbers and personal email addresses as well as banking information.
April 2020	US officials reported seeing a surge of attacks by Chinese hackers against healthcare providers, pharmaceutical manufacturers, and the **US Department of Health and Human Services** amidst the COVID-19 pandemic.
December 2018	Hundreds of gigabytes of data stolen from computers of more than 45 technology companies and US Government agencies. Also stole names, SSNs, DOBs, salary info, phone numbers, and email addresses of more than 100,000 **US Navy** personnel.
September 2018	Since 2014, Starwood hotel chain network breach with estimated personal information of up to 500 million people stolen. Exposed an unusually broad array of data including names, addresses, phone numbers, passport numbers, and credit card numbers, as well as information on where people traveled and with whom.
March 2017	PII of hundreds of millions of people (potentially 143 million) stolen from Equifax, one of the credit reporting agencies that assess the financial health of nearly everyone in the United States.
May 2015	Significant amounts of customer data stolen from United Airlines.
February 2015	Anthem/Blue Cross Blue Shield hack compromised the sensitive personal information of approximately 78.8 million Americans.
April 2015	**OPM** discovered its networks infiltrated and personal information of federal employees, including security clearance information, stolen.
November 2014	**US Postal Service** computer networks breached and data of approximately 800,000 employees exfiltrated.
August 2014	**US Investigations Services** network infiltrated. One of the first steps in the 2015 OPM hack. Community Health Systems disclosed its networks infiltrated and personal information from 4.5 million patients stolen.

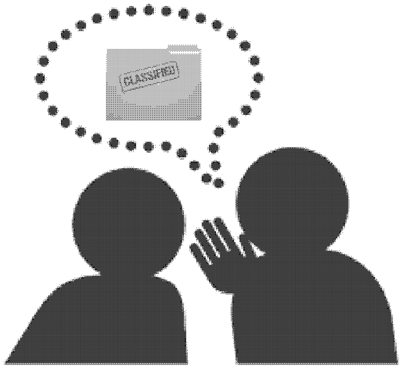
Unauthorized Disclosure - Leaks

- More workers have access to more information

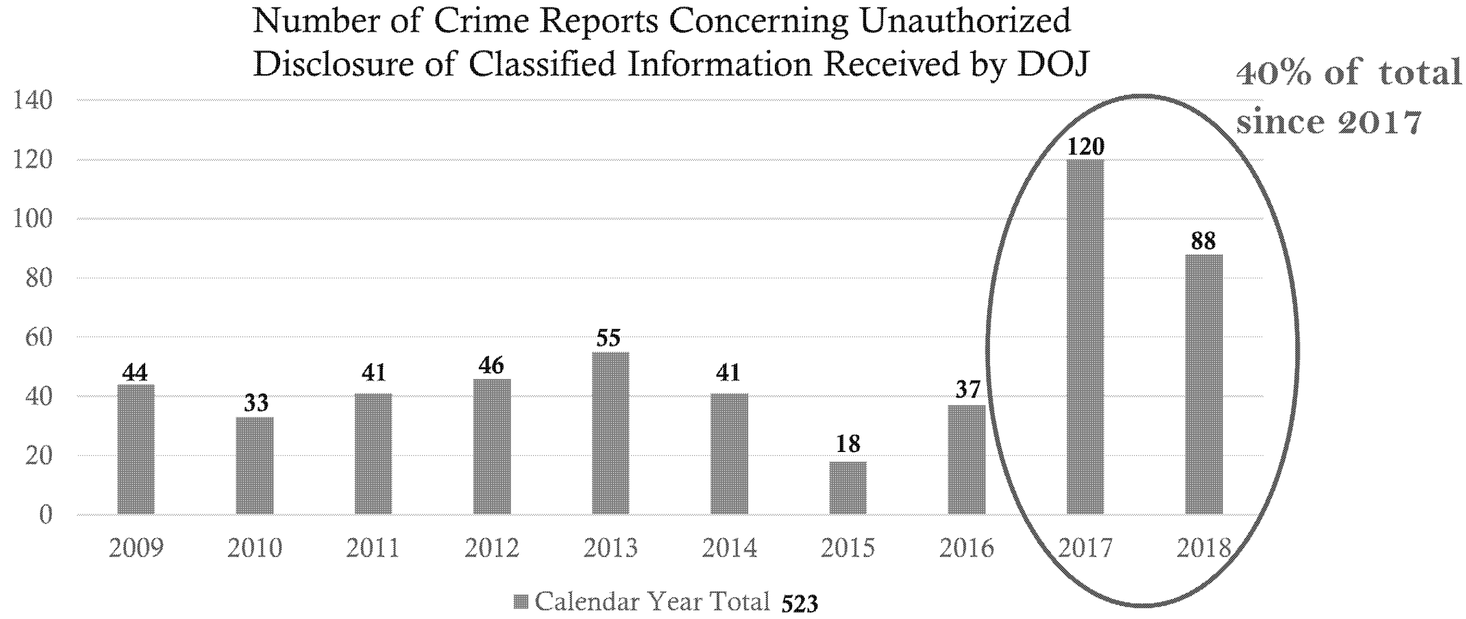
- Non-state actors pose significant threat

"Rise of the Leaktivists"

- Motivations – non-monetary/ financial (disgruntlement, ideology, ego, thrill-seeking)

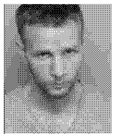
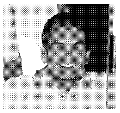
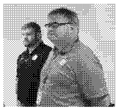
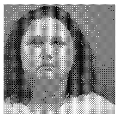
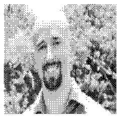
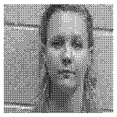


Unauthorized Disclosure – Investigations

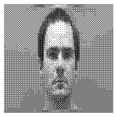
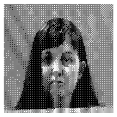
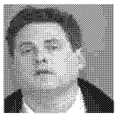


https://fas.org/irp/agency/doj/crimes-reports-2016.html
https://fas.org/irp/agency/doj/crimes-reports.html
https://fas.org/irp/agency/doj/crimes-reports-2017-18.pdf

Recent Unauthorized Disclosure (Leaks) Arrests

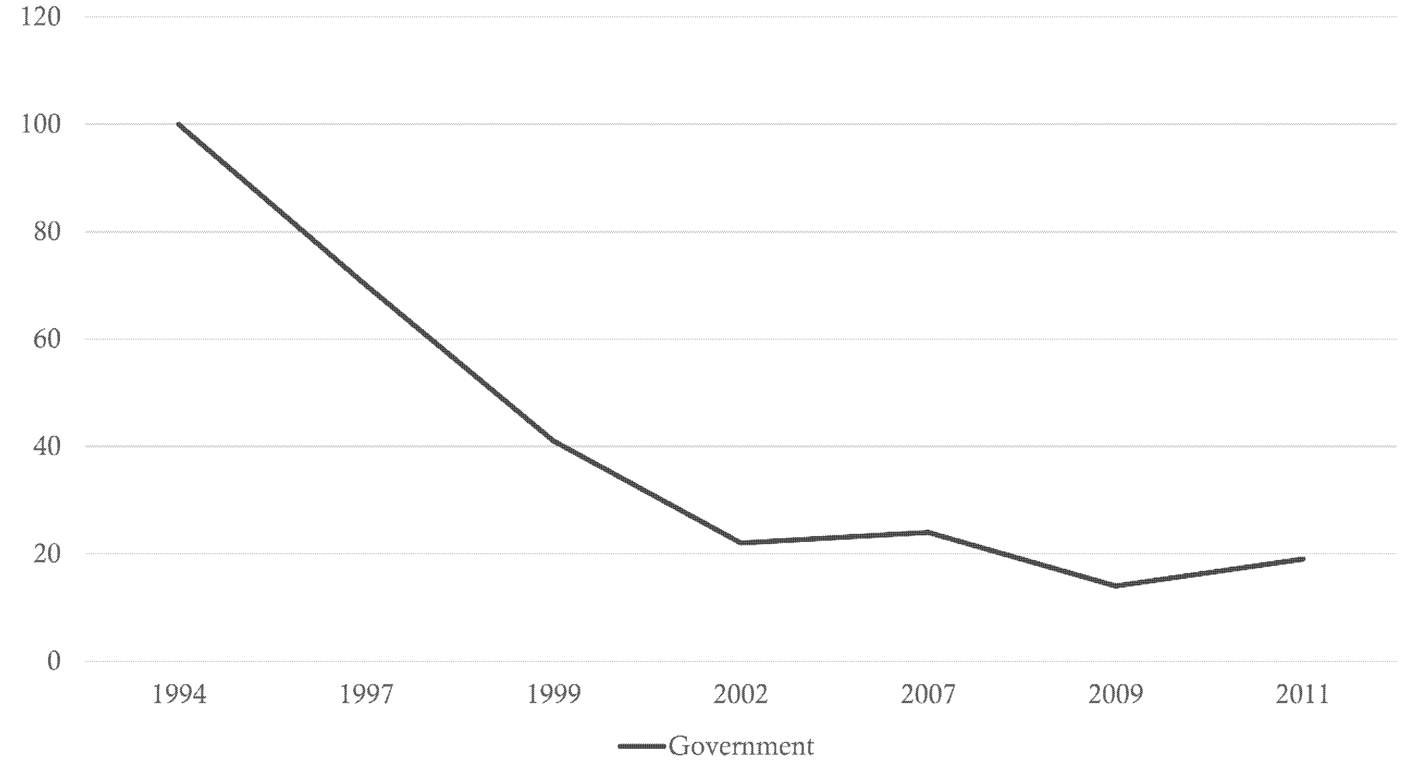
Name	Year of Activity	Provided To	Motivation
 Daniel Everette Hale NGA (contractor)	2013 - 2014	The Intercept	Political? Personal?
 Henry Kyle Freese DIA	2019	NBC, CNBC	Personal Relationship
 John Fry IRS	2018	Michael Avennati, The New Yorker	Political
 Natalie Sours Edwards Department of Treasury	2017 - 2018	BuzzFeed	Political
 Joshua Schulte CIA (contractor)	2017	WikiLeaks	Political Disgruntlement
 Reality Winner NSA (contractor)	2017	The Intercept	Political

Other Unauthorized Disclosure Arrests

Name	Year of Activity	Provided To	Motivation
 Itzaak Vincent Kemp AFRL/NASIC (contractor)	2016 - 2019	???	???
 Elizabeth Jo Shirley NSA, ONI, DOE, DOD, NCIJTF, DOD contractors	1994 - 2002	???	Planned to offer to Russian Government officials in Mexico for help to resettle her and her daughter in Russia
 Harold Thomas Martin NSA (contractor)	~2014 - 2016	???	???

Workplace violence

Rate of nonfatal workplace violence against US Government employees, 1994-2011

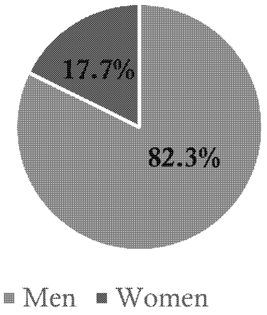


Bureau of Justice Statistics, "*Workplace Violence Against Government Employees,*" *April 2013*

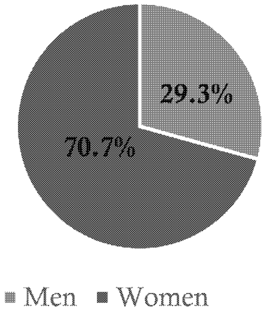
Assaults in US Workplace, 2011-2018

	2011	2012	2013	2014	2015	2016	2017	2018
Total	12,158	13,255	14,204	16,389	16,577	17,390	18,858	21,243
Non-fatal	11,690	12,780	13,800	15,980	16,160	16,890	18,400	20,790
Fatal	468	475	404	409	417	500	458	453

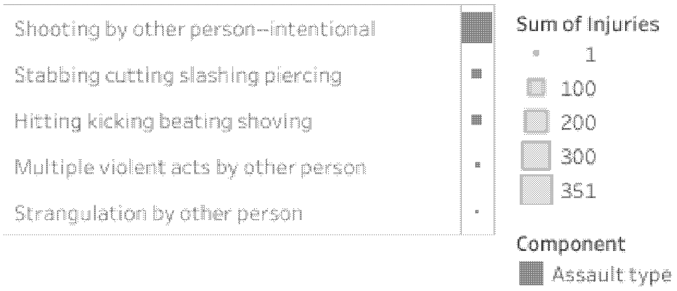
2018 Fatal



2018 Non-fatal



Assault type 2018 Fatal



National Safety Council
https://injuryfacts.nsc.org/work/safety-topics/assault/

Workplace Violence Motivations

- Non-Robbery (eg, interpersonal or work-related argument) increased while Robbery decreased from 2011 - 2015

Robbery Motivation

1990s/early 2000s	65%
2015	46%

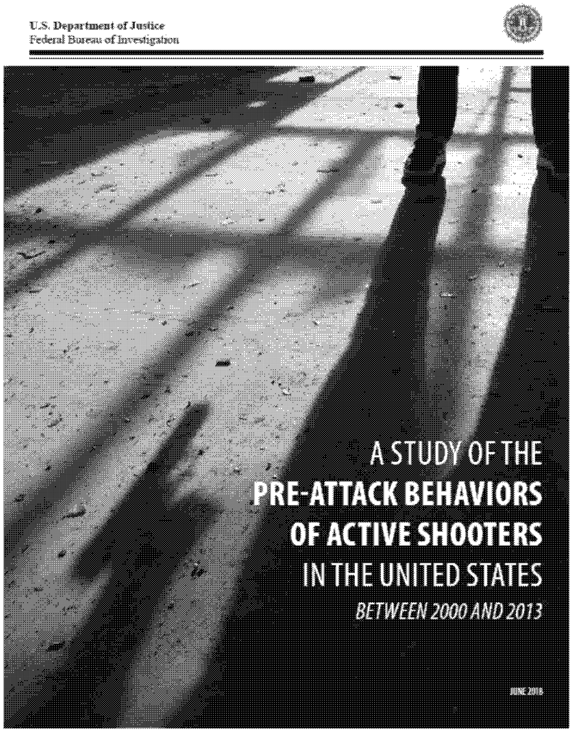
Mitchell L. Doucette, "*What Does Data Tell Us About Trends Workplace Homicides,*" Biomedcentral Blog, 19 March 2019 *https://blogs.biomedcentral.com/on-health/2019/03/19/data-tell-us-trends-workplace-homicides/*

Mitchell L. Doucette, *"Workplace Homicides Committed by Firearm: Recent Trends and Narrative Text Analysis,"* Injury Epidemiology, 18 March 2019

Pre-Attack Behaviors of Active Shooters

Key Findings:

- Active shooters were typically experiencing (an average of 3.6 separate **stressors**) in year before they attacked
- On average, each shooter displayed 4 to 5 **concerning behaviors** over time observable to others around shooter
  - Most frequent related to mental health, problematic interpersonal interactions, and leakage of violent intent
- Most common grievance were related to **adverse interpersonal or employment action** (49%)

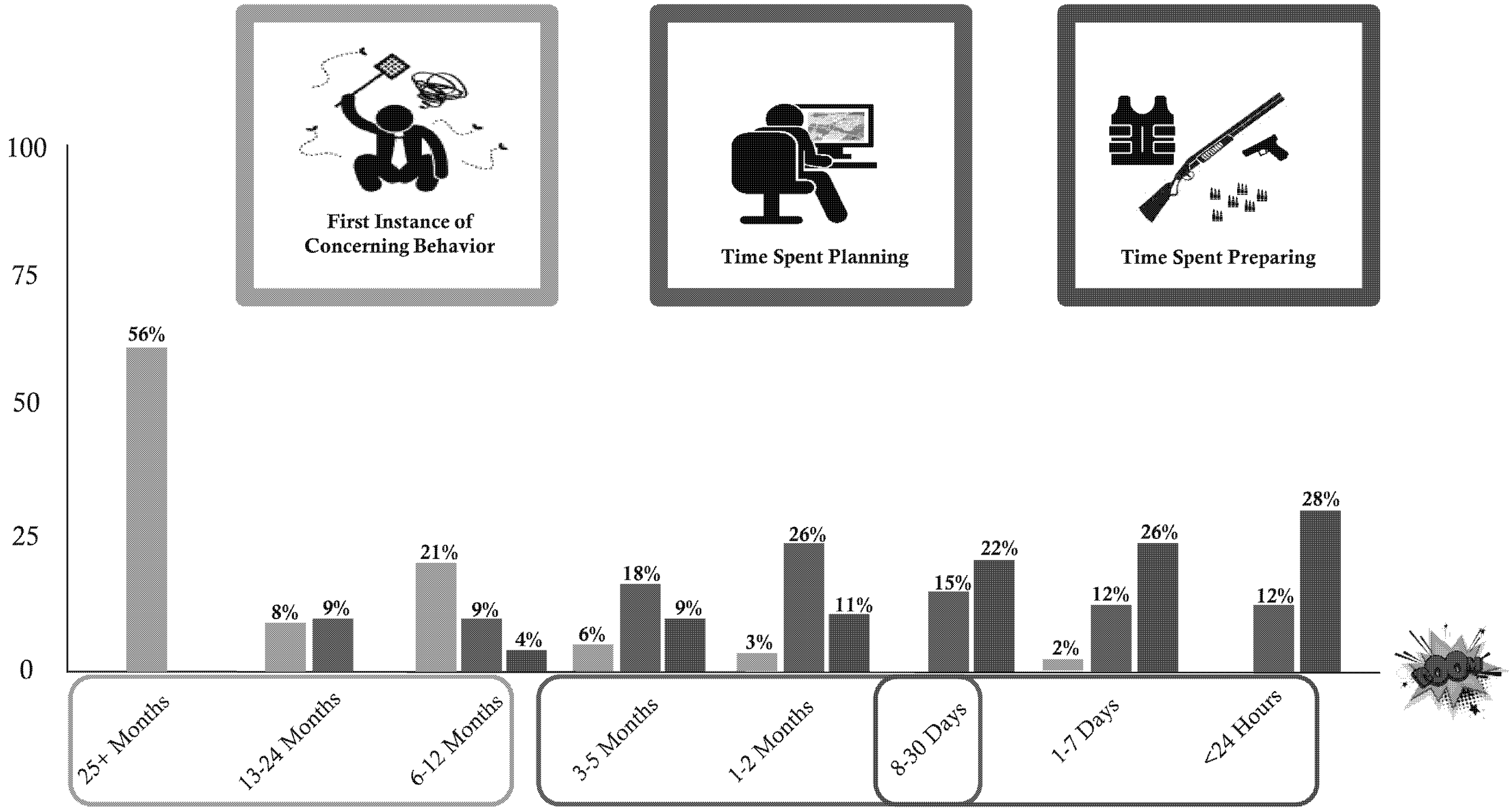


U.S. Department of Justice
Federal Bureau of Investigation

A STUDY OF THE
PRE-ATTACK BEHAVIORS
OF ACTIVE SHOOTERS
IN THE UNITED STATES
BETWEEN 2000 AND 2013

JUNE 2018

https://www.fbi.gov/file-repository/pre-attack-behaviors-of-active-shooters-in-us-2000-2013.pdf/view

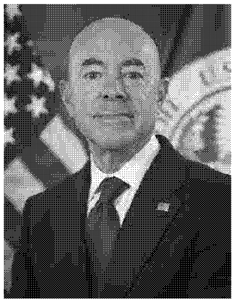

First Instance of Concerning Behavior
Time Spent Planning
Time Spent Preparing
100
75
50
25
0
56%
8%
9%
21%
9%
4%
6%
18%
9%
3%
26%
11%
15%
22%
2%
12%
26%
12%
28%
25+ Months
13-24 Months
6-12 Months
3-5 Months
1-2 Months
8-30 Days
1-7 Days
<24 Hours
BOOM

Violent Domestic Extremism

What the Big Dudes Say

"Domestic violent extremism poses the most lethal and persistent terrorism-related threat to our country today…. I have designated domestic violent extremism as a National Priority Area for the first time…. The Jan. 6 attack on the Capitol was one of many events that constitute a multi-year pattern of violence by domestic extremists."

DHS Secretary Alejandro M. Mayorkis, Washington Post, "*Opinion: Alejandro Mayorkas: How my DHS will combat domestic extremism,*" 25 February 2021



"That attack [6 January 2021 attack on the US Capitol], that siege, was criminal behavior. It is behavior that we, the FBI, view as domestic terrorism….The problem of domestic terrorism has been metastasizing across the country for a long time now and it's not going away anytime soon."

FBI Director Christopher Wray Congressional testimony, 2 March 2021

What US Government/Military Organizations Say

The IC assesses that domestic violent extremists (DVEs) who are motivated by a range of ideologies and galvanized by recent political and societal events in the United States pose an elevated threat to the Homeland in 2021.... The IC assesses that racially or ethnically motivated violent extremists (RMVEs) and militia violent extremists (MVEs) present the most lethal DVE threats, with RMVEs most likely to conduct mass-casualty attacks against civilians and MVEs typically targeting law enforcement and government personnel and facilities.

ODNI, *"Domestic Violent Extremism Poses Heightened Threat in 2021,"* 1 March 2021

"It appears the contemporary movement may be growing as antifa groups recruit followers on fears that fascism is making new inroads in the United States. Such expansion and the rising number of run-ins between antifa supporters and their opponents at public rallies raise the public profile of antifascism in the United States."

Congressional Research Service, *"Antifa—Background,"* 1 March 2018

Antigovernment extremists, specifically those tied to militias, racially or ethnically motivated, or "citing partisan political grievances will likely pose the greatest domestic terrorism threats in 2021."

FBI-DHS Joint Intelligence Bulleting, 2 March 2021

"The primary terrorist threat inside the United States will stem from lone offenders and small cells of individuals, including Domestic Violent Extremists (DVEs).... Among DVEs, racially and ethnically motivated violent extremists—specifically white supremacist extremists (WSEs)—will remain the most persistent and lethal threat in the Homeland....Another motivating force behind domestic terrorism that also poses a threat to the Homeland is anti-government/anti-authority violent extremism.

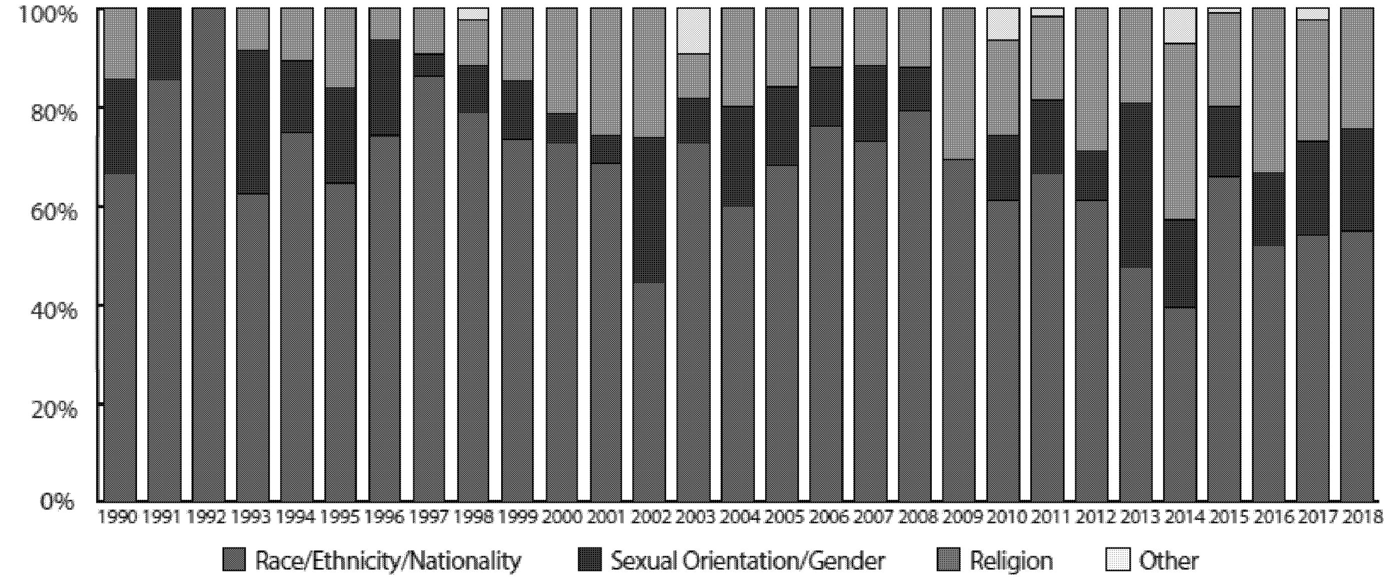
DHS Homeland Threat Assessment, October 2020

"DoD is facing a threat from domestic extremists (DE), particularly those who espouse white supremacy or white nationalist ideologies. Some domestic extremist/terror groups (a) actively attempt to recruit military personnel into their group or cause, (b) encourage their members to join the military, or (c) join, themselves, for the purpose of acquiring combat and tactical experience. Military members are highly prized by these groups as they bring legitimacy to their causes and enhance their ability to carry out attacks."

PERSEREC, *"Leveraging FBI Resources to Enhance Military Accessions Screening and Personnel Security Vetting,"* June 2020

Motivations and Characteristics of Hate Crime Offenders

BIAS Motivations by Year, 1990-2018



"Bias towards individuals on the basis of race, ethnicity, or nationality is the most prevalent category….Offenders motivated by bias on religion and sexual orientation are the second and third most common motivations….From 2013-2018, the data show an increase in the number of offenders with these motivations."

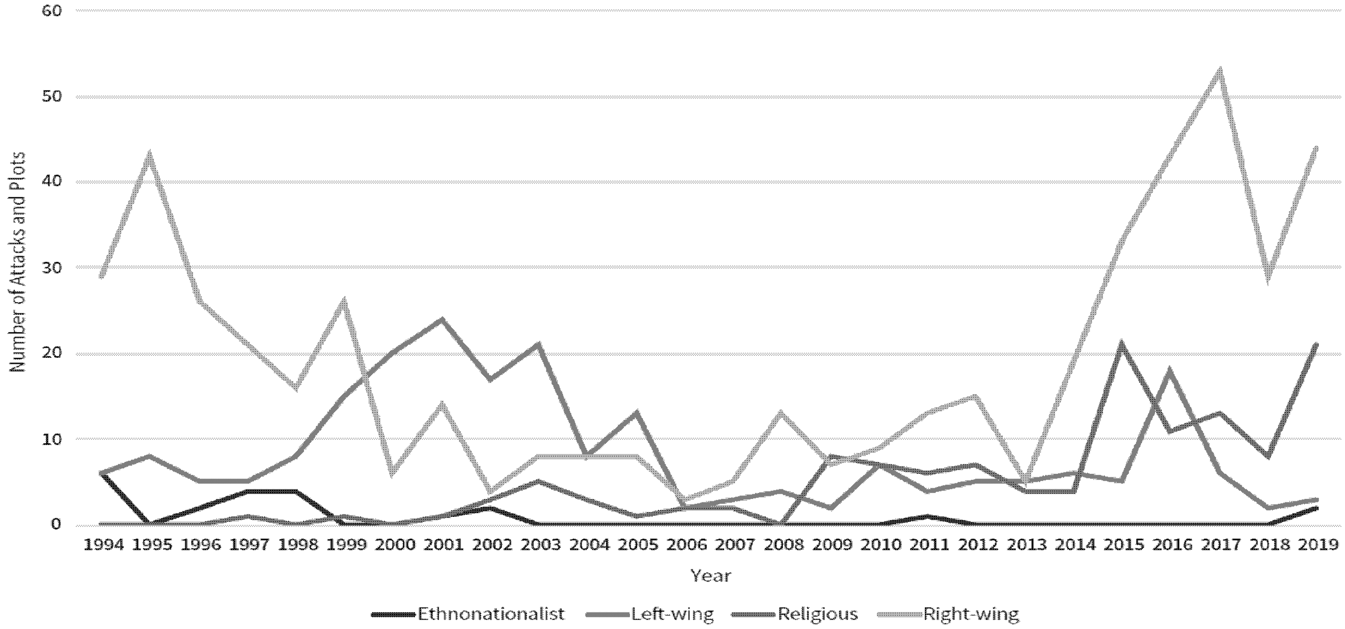
START/University of Maryland, *"Motivations and Characteristics of Hate Crime Offenders,"* October 2020

The Escalating Terrorism Problem in the United States

Center for Strategic and International Studies (CSIS)

June 2020

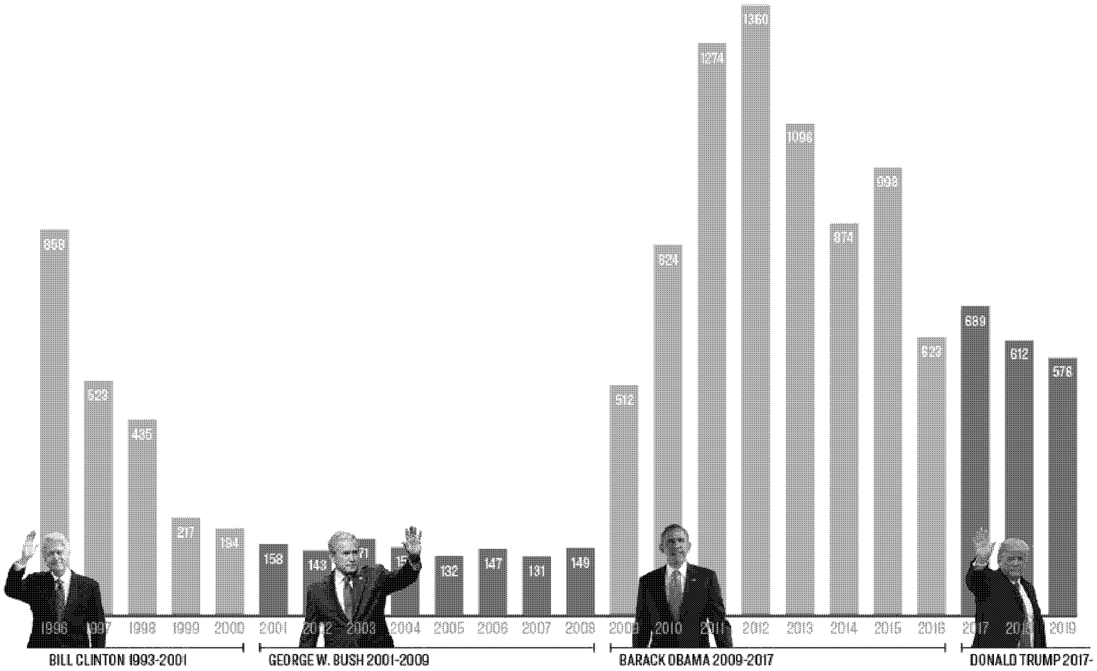
Figure 2: Number of Terrorist Attacks and Plots by Perpetrator Orientation, 1994-2019



"Between 1994 and 2020, there were 893 terrorist attacks and plots in the United States. Overall, right-wing terrorists perpetrated the majority—57 percent—of all attacks and plots during this period, compared to 25 percent committed by left-wing terrorists, 15 percent by religious terrorists, 3 percent by ethnonationalists, and 0.7 percent by terrorists with other motives."

Anti-Government Groups

ANTIGOVERNMENT 'PATRIOT' GROUPS 1995–2019



Southern Poverty Law Center
https://www.splcenter.org/fighting-hate/extremist-files/ideology/antigovernment

QAnon

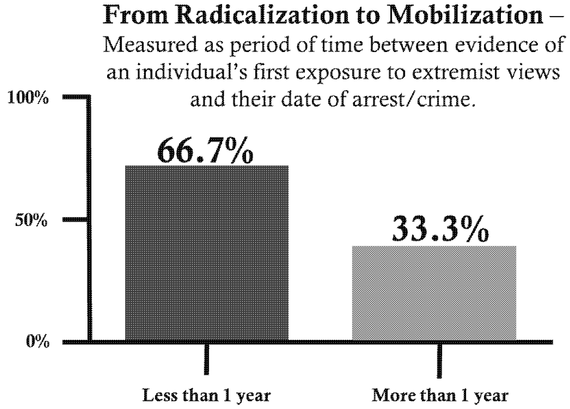
- As of 24 February 2021, 56 QAnon followers have committed ideologically-motivated crimes in the US—including 27 who have participated in the 6 January 2021 attack on the US Capitol

- Women were 19% of non-Capitol offenders and 24% of Capitol rioters

- Sixty-eight (68%) percent of non-Capitol offenders have documented mental health concerns—these include post-traumatic stress disorder, paranoid schizophrenia, bipolar disorder, and Munchausen syndrome by proxy—according to court records and other public sources

- Forty-four (44%) percent on non-Capitol offenders radicalized after experiencing a traumatic event—premature deaths of loved ones; physical, emotional, or sexual abuse; post-traumatic stress disorder from military service
    - 83% of women non-Capitol offenders experienced trauma which involved physical and/or sexual abuse of their children by a romantic partner or family member

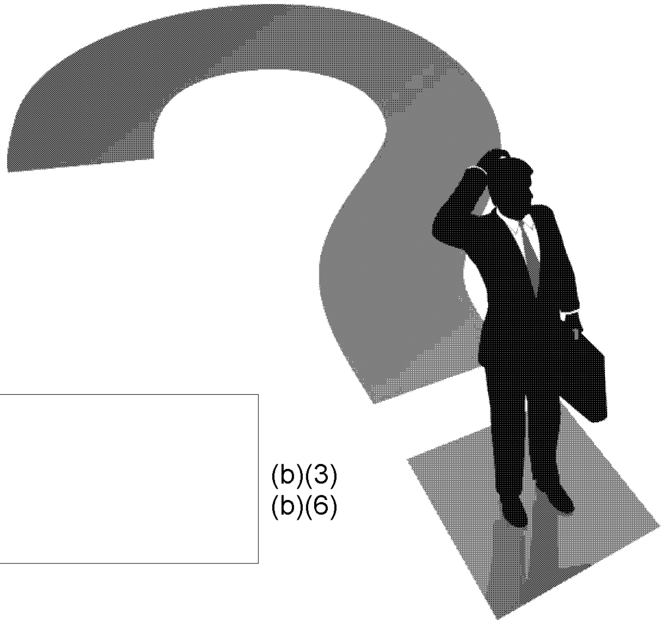
- While some extremists radicalize over extended periods of time, data indicates the majority radicalized in less than a year, and some in mere weeks



From Radicalization to Mobilization – Measured as period of time between evidence of an individual's first exposure to extremist views and their date of arrest/crime.

START/University of Maryland, *"QAnon Offenders in the United States,"* February 2021

Questions?



[redacted]

(b)(3)
(b)(6)