ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

March 29, 2023

ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY

Office of the Director of National Intelligence | February 6, 2023

This annual report of worldwide threats to the national security of the United States responds to Section 617 of the FY21 Intelligence Authorization Act (Pub. L. No. 116-260). This report reflects the collective insights of the Intelligence Community (IC), which is committed every day to providing the nuanced, independent, and unvarnished intelligence that policymakers, warfighters, and domestic law enforcement personnel need to protect American lives and America's interests anywhere in the world. This assessment focuses on the most direct, serious threats to the United States during the next year. The order of the topics presented in this assessment does not necessarily indicate their relative importance or the magnitude of the threats in the view of the IC. All require a robust intelligence response, including those where a near-term focus may help head off greater threats in the future. Information available as of 18 January was used in the preparation of this assessment.

Read the full article here.

OPEN-SOURCE INTELLIGENCE IS INDISPENSABLE FOR COUNTERING THREATS

Eric Mandel and Sarit Zehavi | The National Interest | March 4, 2023

When most people hear the word intelligence in a political context, they immediately think of clandestine sources, spies, and secret meetings. Intelligence services still rely on human source intelligence (HUMINT) and intercepted communications (SIGINT). However, in the twenty-first century, open-source intelligence (OSINT) has become indispensable for understanding your adversaries and is often the primary and most valuable source of actionable intelligence. According to a detailed article highlighting the power of OSINT in the Wall Street Journal, "80% of what a U.S. president or military commander needs to know comes from OSINT." What then is OSINT, and why is it so important in 2023? In brief, OSINT is the painstaking gathering and analysis of information from a wide range of open sources for the military, intelligence, police, and business communities. The explosion of social media—from real-time videos to blogs to chat rooms to Twitter and Facebook—has produced unprecedented opportunities for insight into areas and people where HUMINT and SIGINT are not as effective or cost too much while decreasing the risk to human intelligence assets.

Read the full article here.

US INTEL: CHINESE INFLUENCE OPERATIONS ARE GROWING MORE AGGRESSIVE, MORE SIMILAR TO RUSSIA'S

Elias Groll | CyberScoop | March 8, 2023

U.S. intelligence officials warned on Wednesday that China is stepping up its efforts to carry out influence operations against the United States and that its efforts to influence American public opinion increasingly resemble Russian operations. In testimony before the Senate Intelligence Committee and in the U.S. intelligence community's annual threat assessment published on Wednesday, U.S. intelligence leaders cautioned that China represents perhaps the leading threat to U.S. power and that the conflict between Washington and Beijing is increasingly playing out along technological lines. "The People's Republic of China, which is increasingly challenging the United States economically, technologically, politically and military around the world, remains our unparalleled priority," Director of National Intelligence Avril Haines said during her testimony on Wednesday before the Senate Intelligence Committee during its annual worldwide threats hearing. But Haines also cautioned that Chinese leader Xi Jinping is not eager for a fight with the United States.

Read the full article here.

TIKTOK GENERATION: A CCP OFFICIAL IN EVERY POCKET

Kara Frederick | The Heritage Foundation | March 22, 2023

Every day that TikTok is allowed to operate in the United States is another day that China can collect data on American citizens and sharpen its ability to exploit them—especially young people. The more that TikTok becomes embedded in U.S. society, the harder it will be to uproot. Even so, there will be another TikTok. Without implementing a systemic, risk-based framework to proactively address the next TikTok now, the U.S. will have ceded yet another critical digital battlespace to its adversaries. More so, U.S. policymakers have a duty to safeguard America's social fabric and protect young citizens from the whims of a hostile, foreign nation. Failing to deliver means that the next generation of Americans will pay the price for Washington's lassitude. Three hundred billion dollars, three billion downloads, and at least 90 minutes of attention per user every day—TikTok and its China-based parent company have captured much of the world in more ways than one. Yet today's most popular social media app poses a distinct threat to American citizens.

Read the full article here.

CAN CHIPS AND SCIENCE ACHIEVE ITS POTENTIAL?

Matt Hourihan | Issues in Science and Technology | Winter 2023

Amid rising concerns over the United States' capacity to innovate and address large-scale societal challenges, the CHIPS and Science Act represents a positive and well-timed achievement for legislators and their staff. As multiple authors point out in a special section of the Fall 2022 Issues that explores how to help the act deliver on its promises, the 400-page law seeks to address goals in a variety of areas: semiconductor production; skills development in science, technology, engineering, and mathematics; regional innovation, and discovery science, among others. In "An Infection Point for Technological Leadership?" Steven C. Currall and Venkatesh Narayanamurti raise a particularly salient and subtle point: the attempt in CHIPS to nudge parallel investments in discovery science and technological invention, primarily through reforms to the National Science Foundation. The intimate interplay between discovery and invention has yielded breakthroughs in the past, and such linked investments may offer potential going forward. Even before CHIPS, the NSF boasted an appealing mix of discovery science grant programs, multidisciplinary research centers, and industrial partnerships.

Read the full article here.

AMID STRAINED US TIES, CHINA FINDS UNLIKELY FRIENDS IN UTAH

Alan Suderman and Sam Metz | AP News | March 27, 2023

China's global campaign to win friends and influence policy has blossomed in a surprising place: Utah, a deeply religious and conservative state with few obvious ties to the world's most powerful communist country. An investigation by The Associated Press has found that China and its U.S.-based advocates spent years building relationships with the state's officials and lawmakers. Those efforts have paid dividends at home and abroad, the AP found: Lawmakers delayed legislation Beijing didn't like, nixed resolutions that conveyed displeasure with its actions and expressed support in ways that enhanced the Chinese government's image. Its work in Utah is emblematic of a broader effort by Beijing to secure allies at the local level as its relations with the U.S. and its western allies have turned acrimonious. U.S. officials say local leaders are at risk of being manipulated by China and have deemed the influence campaign a threat to national security.

Read the full article here.

PALL OF SUSPICION

Jeffrey Mervis | Science | March 23, 2023

For decades, Chinese-born U.S. faculty members were applauded for working with colleagues in China, and their universities cited the rich payoff from closer ties to the emerging scientific giant. But those institutions did an about-face after they began to receive emails in late 2018 from the U.S. National Institutes of Health (NIH). The emails asked some 100 institutions to investigate allegations that one or more of their faculty had violated NIH policies designed to ensure federal funds were being spent properly. Most commonly, NIH claimed a researcher was using part of a grant to do work in China through an undisclosed affiliation with a Chinese institution. Four years later, 103 of those scientists—some 42% of the 246 targeted in the letters, most of them tenured faculty members—had lost their jobs. In contrast to the very public criminal prosecutions of academic scientists under the China Initiative launched in 2018 by then-President Donald Trump to thwart Chinese espionage, NIH's version has been conducted behind closed doors.

Read the full article here.

CONCERN OVER TIKTOK NOT JUST ABOUT DATA, BUT ALSO ITS ALGORITHM AND PUSHING OF CERTAIN MESSAGING: US CYBER COMMAND CHIEF

Fabian Koh | CNA | March 24, 2023

Cyber warfare methods are increasingly sophisticated, and it takes immense preparation and the sharing of information to fend off attacks, the head of the United States cyber command said on Friday (Mar 24). Speaking to CNA on the sidelines of the Singapore Defence Technology Summit 2023, General Paul Nakasone, commander of the US Cyber Command and director of the National Security Agency (NSA), added that the US is concerned with dual-use technology, such as artificial intelligence (AI), being used to impede free speech. He said that apart from the data collected, social media apps like TikTok are a concern, as their unique algorithms could be used to push certain messaging. The three-day event brought together representatives from government, industry and academia to discuss developments in defence and security capabilities. General Nakasone said that dual-use technology, such as AI and machine learning, provides both a great opportunity and challenge, and countries should be able to recognise it, adapt quickly to it and employ it in various ways. Citing influence operations, he said that AI could be used to push a certain narrative, or to influence a particular leaning on a policy or an election.

Read the full article here.

COLLABORATIVE ADVANTAGE: CREATING GLOBAL COMMONS FOR SCIENCE, TECHNOLOGY, AND INNOVATION

Leonard Lynn and Hal Salzman | Issues in Science and Technology | March 6, 2023

What was once described as the "American Century" of political and technological dominance is giving way to a polycentric world. In this new order, the fate of nations will depend on international collaboration for innovation and prosperity, particularly as global challenges including disease, poverty, energy deficits, and climate change threaten all. The innovations needed can no longer be produced by only a few nations, nor can the benefits be confined to those few. Developing such innovations, however, will require collaborative efforts at a global scale that go beyond anything previously attempted. In the postwar decades, the United States pursued a techno-nationalist path in research and development that became a global norm. The US government was capable of funding research projects at far higher levels than other governments; US firms also directed substantial portions of revenue to R&D, extending federal efforts. The world's most advanced R&D laboratories included the largely independent Bell Labs and Xerox PARC, while companies like IBM, GE, RCA, DuPont, and Polaroid were engaged in significant basic and exploratory research.

Read the full article here.

INSIDER THREAT RISK: A BREAKDOWN BY INDUSTRY

Jeff B. Copeland | RiskLens | March 23, 2023

"We have met the enemy and he is us," goes the old joke, never truer than in cyber risk -- Insider Error ranked #2, and Insider Misuse #3 among risk themes for total loss exposure in the RiskLens 2023 Cybersecurity Risk Report (#1 went to Basic Web Application Attacks). Insider Error = Misconfigurations, failures to renew expired certificates, improper publishing and other unintentional errors by staff members that can have damaging consequences to the bottom line. Digital transformation (aka movement to the cloud) has opened new vectors for insider error: The Pentagon Leaked Sensitive Military Emails via a Misconfigured Microsoft Azure Government Cloud. Insider Misuse = Intentional and malicious disclosure or modification of sensitive data by trusted employees, leading to significant loss to the company. Add to the traditional threat actor, the disgruntled insider, a new breed: Employees who sell out to ransomware gangs or other criminals: AT&T Employees Took Bribes to Plant Malware. Our 2023 report enables you to drill down into your industry by risk themes to uncover the most probable frequency and financial impact of loss events. And, if you're in Public Administration or Healthcare, the news is not good.

Read the full article here.

HOW CHINA-LINKED ESPIONAGE IS HINDERING TIKTOK'S U.S. FUTURE

Sam Sabin | Axios | March 24, 2023

TikTok's biggest problem isn't its data security programs, it's the race between the U.S. and China to become the world's dominant cyber superpower. Driving the news: TikTok CEO Shou Zi Chew's testimony before the House Energy and Commerce Committee Thursday did little to sway lawmakers who argue that the Chinese government could harness millions of Americans' TikTok data. But lawmakers also struggled to articulate their main concern behind targeting TikTok: China's espionage capabilities have become sophisticated and harder to detect in recent years. The big picture: Chilling relations between the U.S. government and Beijing have only made lawmakers more wary of the capabilities China-backed hacking teams are brewing — and what classified U.S. data they're collecting. The 2014 hacks of the Office of Personnel Management, which several firms linked to China, opened up the U.S. cyber community's eyes, Bryan Cunningham, former adviser to the White House National Security Council, told Axios.

Read the full article here.

ESF PARTNERS, NSA, AND CISA RELEASE IDENTITY AND ACCESS MANAGEMENT RECOMMENDED BEST PRACTICES FOR ADMINISTRATORS

National Security Agency | Central Security Service | March 21, 2023

As part of the Enduring Security Framework (ESF), the National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA) published the Recommended Best Practices Guide for Administrators to provide system administrators with actionable recommendations to better secure their systems from threats to Identity and Access Management (IAM). IAM is a framework of business processes, policies, and technologies that facilitate the management of digital identities. It ensures that users only gain access to data when they have the appropriate credentials. In 2021, Colonial Pipeline, a major Southeast oil pipeline system, suffered a major ransomware attack, disrupting the oil/gas distribution system and causing long lines at the gas station and consumer panic. Many people know about the attack and the exploitation of the company for money, but many don't realize that the attack happened because of a leaked password, an inactive VPN account, and a lack of multifactor authentication – all of which can be summed up as poor IAM.

Read the full article here.

COUNTERING CHINA REQUIRES A NEW APPROACH TO COUNTERINTELLIGENCE

Greg Levesque and Holden Triplett | The Well News | March 9, 2023

The Chinese balloon moving over the continental United States last month, as we know now, was not some rogue surveillance operation gone wrong. Instead, it was part of a broader surveillance program that China directed over the past few years. This should come as no surprise. China and its leaders are clear about what their national priorities are, and once determined, the country uses all aspects of its military and civilian infrastructure to achieve its goals. That's the case with this surveillance program, and it's also the case with the long-standing effort to steal the intellectual property of U.S.-based companies, particularly in strategic areas including quantum computing, AI, autonomous vehicles, drones or even rare-earth metals and semiconductors. The cost of China's activities against U.S. businesses alone has been pegged at $600 billion a year. The United States finds itself in a multi-front battle with China for both geopolitical and technological dominance. Yet, while China has built a strategic program of Military-Civil Fusion, the U.S., up to this point, has failed to meet the moment.

Read the full article here.

MAINTAINING TECHNOLOGY ADVANTAGE (MTA)

Department of Defense Research & Engineering Enterprise | Science and Technology (S&T) Program Protection

The Science and Technology Program Protection Office's Maintaining Technology Advantage (MTA) Directorate leads Department of Defense (DoD) efforts to balance the promotion and protection of critical and emerging technologies (C&ET) throughout the technology development lifecycle. These MTA efforts ensure that the U.S. maintains worldwide leadership in C&ET, which are foundational to the unquestioned superiority of the American joint forces. MTA collaborates closely with the other elements of the National Security Innovation Base (NSIB) – to include the Military Services, other DoD offices, the U.S. defense industry, and the U.S. academic/research enterprise – to identify and implement best practices, policies, mechanisms, strategies, and standards that protect U.S. technological advantage, foster U.S. technological development, and mitigate exploitation by strategic competitors. The following sections highlight major MTA initiatives and lines of effort.

View the full resource here.

PROTECT YOURSELF: COMMERCIAL SURVEILLANCE TOOLS

National Counterintelligence and Security Center | U.S. Department of State | January 7, 2022

Companies and individuals have been selling commercial surveillance tools to governments and other entities that have used them for malicious purposes. Journalists, dissidents, and other persons around the world have been targeted and tracked using these tools, which allow malign actors to infect mobile and internet-connected devices with malware over both WiFi and cellular data connections. In some cases, malign actors can infect a targeted device with no action from the device owner. In others, they can use an infected link to gain access to a device. These surveillance tools can: record audio, including phone calls, track phone's location, and access and retrieve virtually all content on a phone, including text messages, files, chats, commercial messaging app content, contacts, and browsing history. Below are common cybersecurity practices that may mitigate some risks.

View the full resource here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Academic Security and Counter Exploitation Program is coordinated by The Texas A&M University System Research Security Office as a service to the academic community.
https://rso.tamus.edu