МЕЖДУНАРОДЕН ОБРАЗОВАТЕЛЕН ФОРУМ
''ОБРАЗОВАНИЕТО ПРЕЗ ПАРАДИГМАТА НА ХУМАНИЗМА И ИЗКУСТВЕНИЯ ИНТЕЛЕКТ''

ИЗКУСТВЕНИЯТ ИНТЕЛЕКТ И РОЛЯТА МУ В ЗАЩИТА НА КИБЕРПРОСТРАНСТВОТО

ДИМИТЪР ДИМИТРОВ
ВИСШЕ ВОЕННОМОРСКО УЧИЛИЩЕ „НИКОЛА ВАПЦАРОВ“

Въведение в настоящия пейзаж на заплахите. Киберпространството като основен стратегически метод за конкуриране между Великите Сили

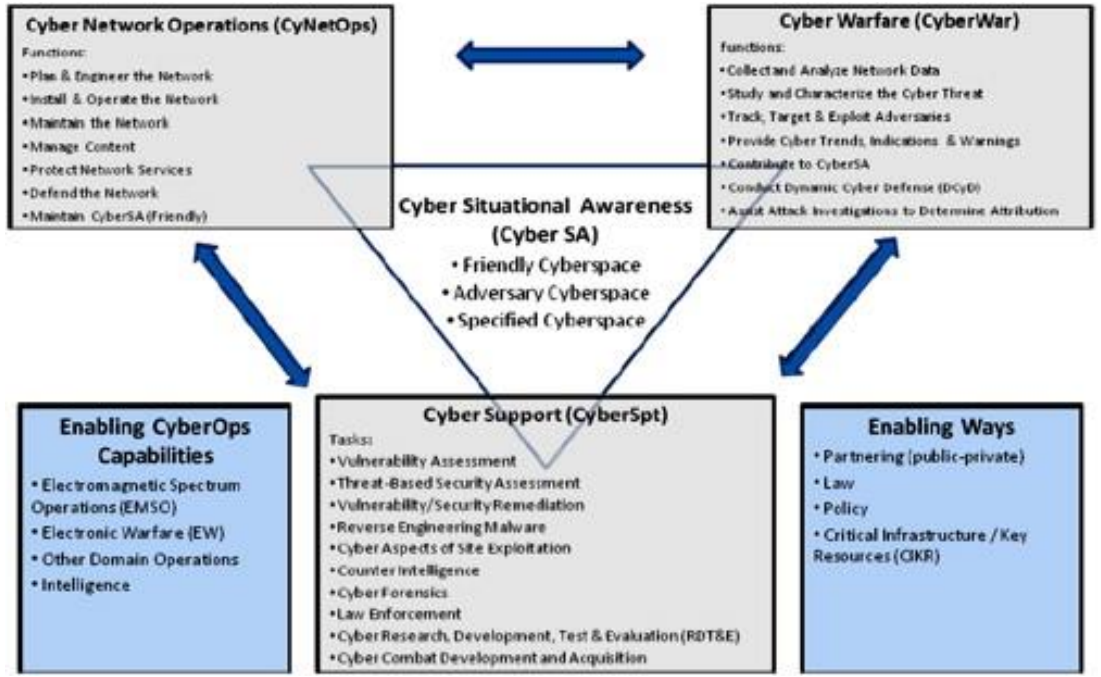
Киберпространството действа като главно бойно поле за прилагането на новите доктринални идеи за постигане на възпиращи операции

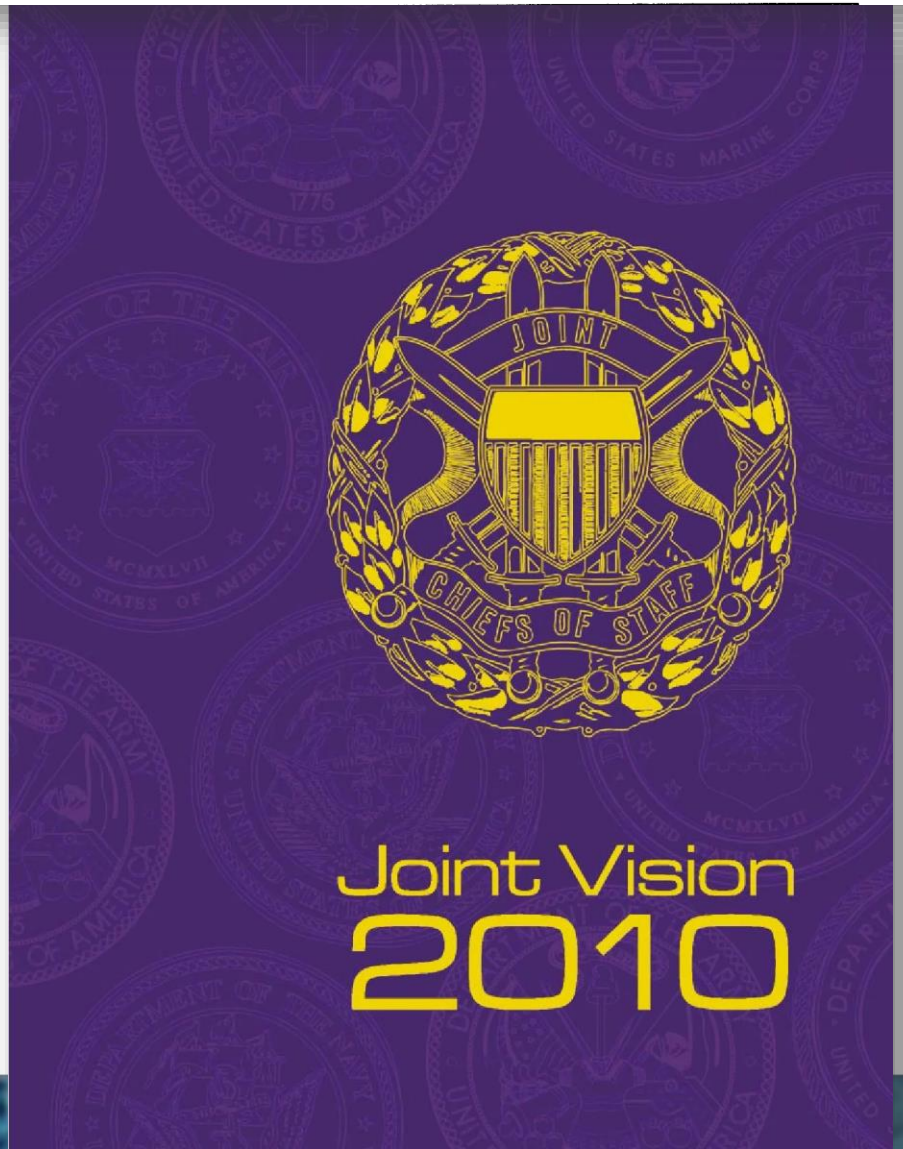
Стратегическото водене на съревнование между Великите Сили е основано на идеята за доминиране в киберпрстранството

Our current **National Military Strategy** (NMS), dated September 1997, classifies information warfare as a "special concern" under the heading of Asymmetric Challenges.[29] In addition to identifying information superiority as a key enabler for Joint Vision 2010, the NMS also states: "Joint Vision 2010 rests on the foundations of information superiority and technological innovation."[30] The NMS expands upon the Joint definition of information superiority by specifying:

Основи, поставени през 90те – Обединена визия 2010

Бащата на TAO - James R. Gosler, Кръстникът на американската кибервойна



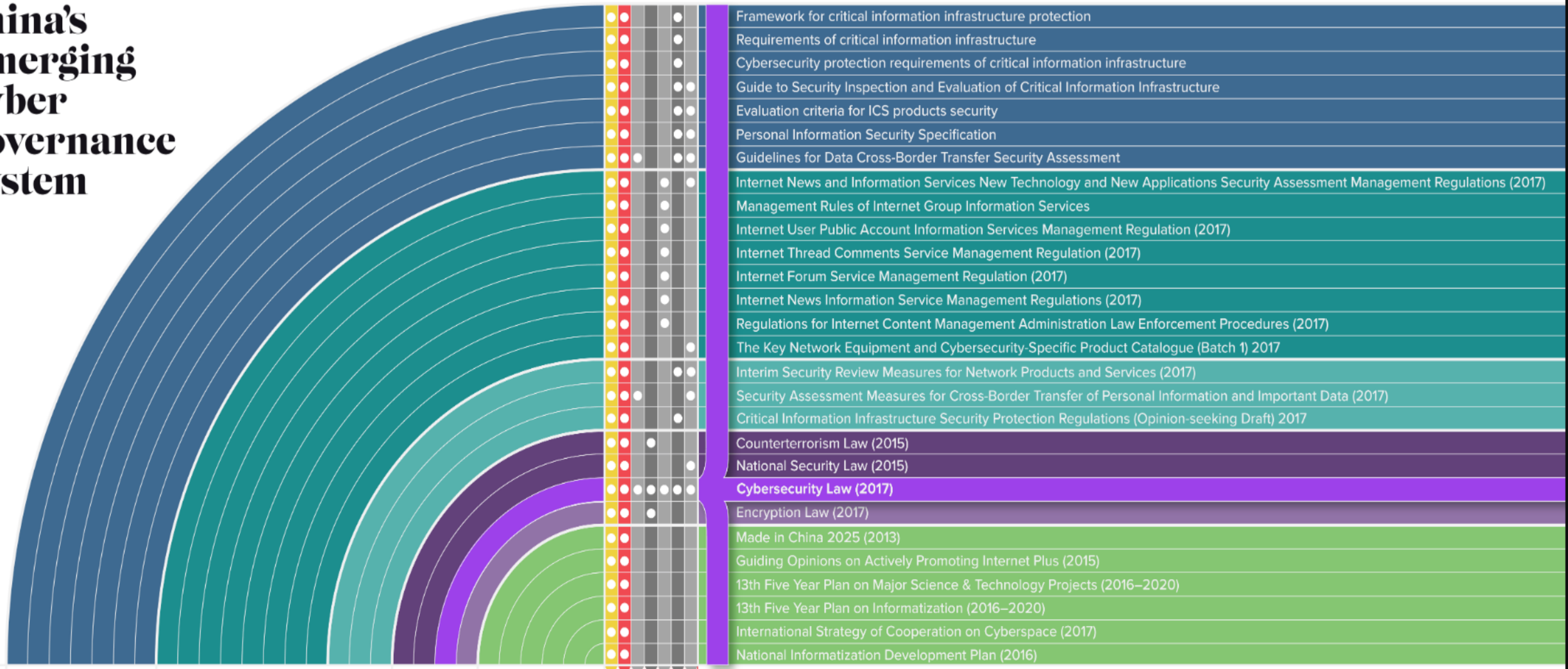


Най – яркия пример за стратегически важно разбиране на киберпорстранството като основен източник на възпиране, освен САЩ, е може би Китай.

Чрез включването и възприемането на киберпространството като неразделен компонент на военната си доктрина Китай продължава своята активна отбрана и работи за междувременното ускоряване на революцията за военното дело.

Тези всеобхватни усилия за управление и регулиране на информационния поток се характеризират като "информатизирана военна революция".

China's Emerging Cyber Governance System



CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

China blamed as major backer behind hacking of Australian companies and infrastructure

By political reporter Matthew Doran

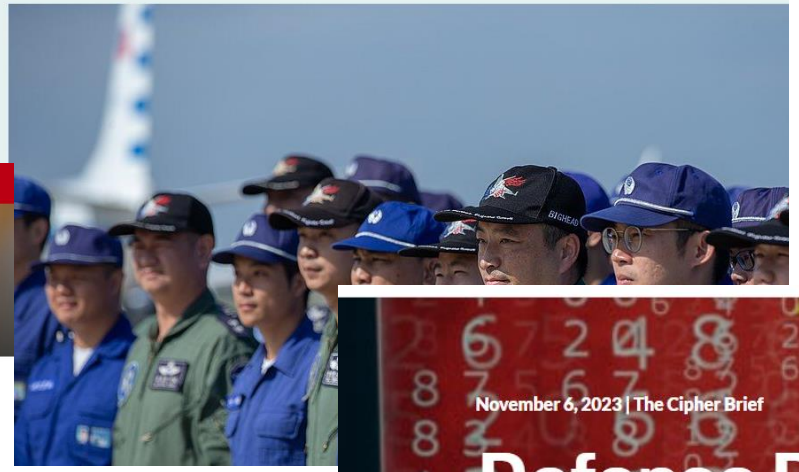
Posted 16h ago, updated 9h ago

Armed Conflict | Cybersecurity & Tech | Foreign Relations & International Law

Securing Taiwan's Satellite Infrastructure Against China's Reach

Gil Baram | Tuesday, November 14, 2023, 10:14 AM

As Taiwan faces the looming threat of a Chinese invasion, the need to fortify its satellite infrastructu becomes ever more urgent.



China

U.S. warns China could hack infrastructure, including pipelines, rail systems

By **Raphael Satter**, **Zeba Siddiqui** and **James Pearson**

May 26, 2023 12:05 PM GMT+3 · Updated 6 months ago

May 25 (Reuters) - The U.S. State Department warned on Thursday that China was capable of launching cyber attacks against critical infrastructure, including oil and gas pipelines and rail systems, after researchers discovered a Chinese hacking group had been spying on such networks.

A multi-nation alert issued Wednesday revealed the Chinese cyber-espionage campaign had been aimed at military and government targets in the United States.

The Chinese government has rejected assertions that its spies are going after Western targets, calling the warning issued by the United States and its allies a "collective disinformation campaign."

U.S. officials said they were still in the process of getting their arms around the threat.

"We've had at least one location that we didn't know about since the hunt guide was released come forward with data and information," Rob Joyce, the U.S. National Security Agency's (NSA) cybersecurity director, told Reuters. The agency disclosed technical details earlier to help critical service providers detect

News | Topics | Features | Webinars | White Papers | Podcasts | Events & Conferences | Directory

NEWS 5 OCT 2023

China Poised to Disrupt US Critical Infrastructure with Cyber-Attacks, Microsoft Warns

James Coker

Deputy Editor, Infosecurity Magazine

Follow @ReporterCoker

Chinese threat actors are positioning themselves to deploy major cyber-attacks against US critical national infrastructure (CNI) in the event of an escalation of hostilities between the two nations.

Microsoft's latest Digital Defense Report (MDDR) observed a rise in Chinese state-affiliated actors, such as Circle Typhoon and Volt Typhoon, targeting sectors like transportation, utilities, medical infrastructure and telecommunications.

These campaigns may be intended to enable China to disrupt critical infrastructure

You may also like

NEWS 8 OCT 2021

Microsoft: Russia Dominates State-Sponsored Attacks

NEWS 16 FE

Microsoft: 1(SolarWinds

Democracy Dies in Darkness

November 6, 2023 | The Cipher Brief

Defense Department Report Highlights Cyber Threat from China

RADM (Ret.) Mark Montgomery

CCTI Senior Director and Senior Fellow

Jiwon Ma

Program Analyst

top EXCLUSIVE

China hacked Japan's sensitive defense networks, officials say

Tokyo has strengthened its defenses after a major cybersecurity breach, but gaps remain that could slow info sharing with the Pentagon

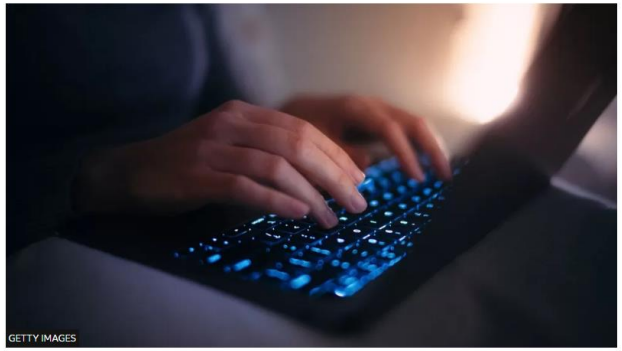
By Ellen Nakashima

Updated August 8, 2023 at 2:36 a.m. EDT | Published August 7, 2023 at 3:26 p.m. EDT

Asia | China | India

Microsoft: Chinese hackers hit key US bases on Guam

25 May



Chinese hackers are accused of breaching US military bases on Guam

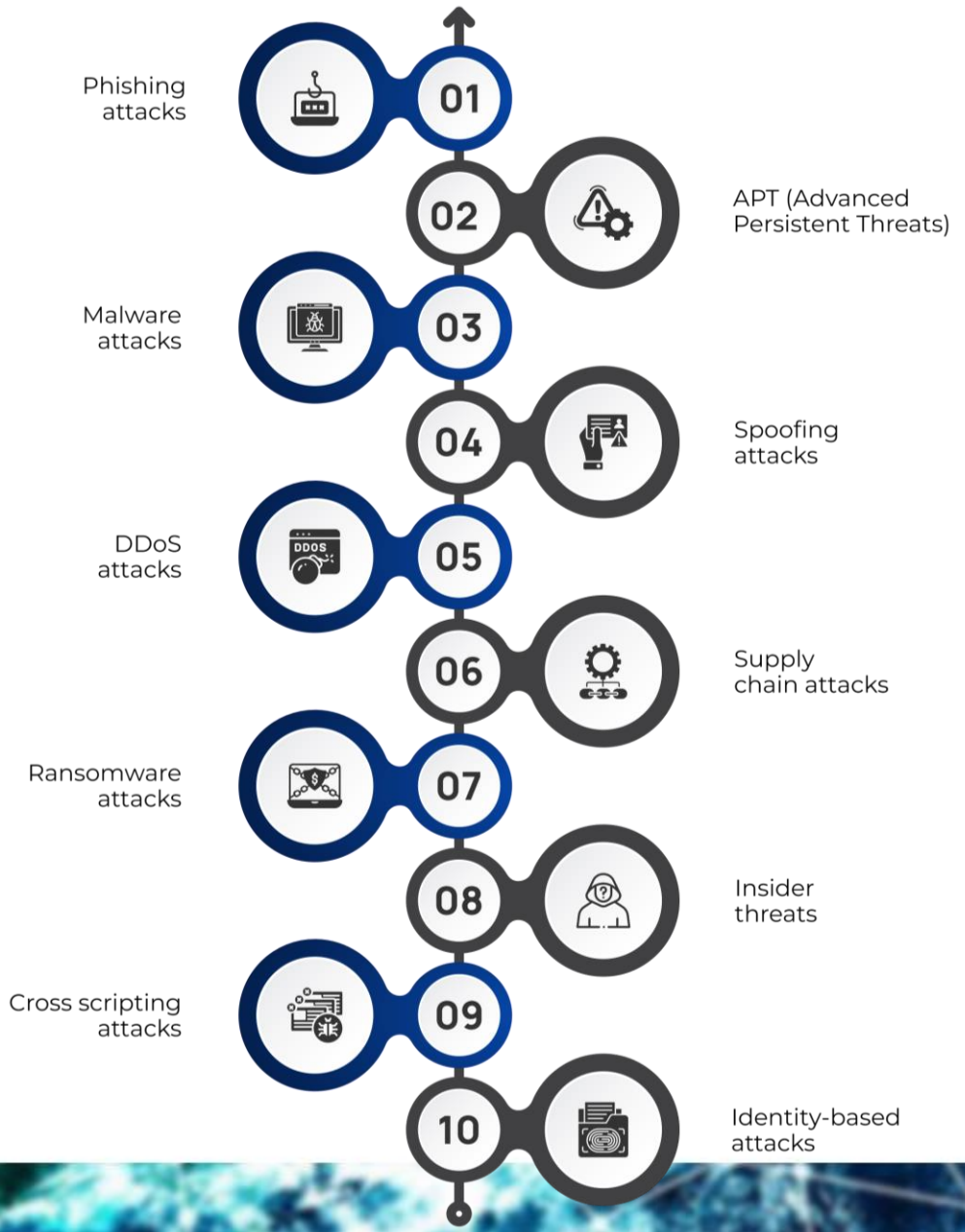
By Hannah Ritchie

BBC News

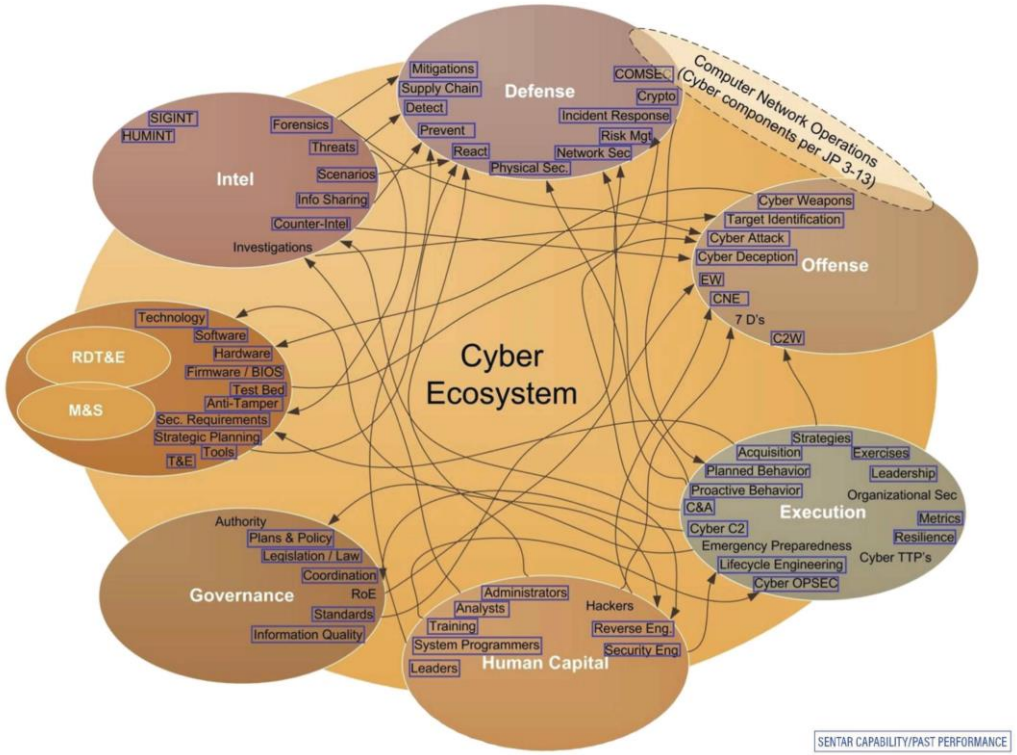
en to analysis

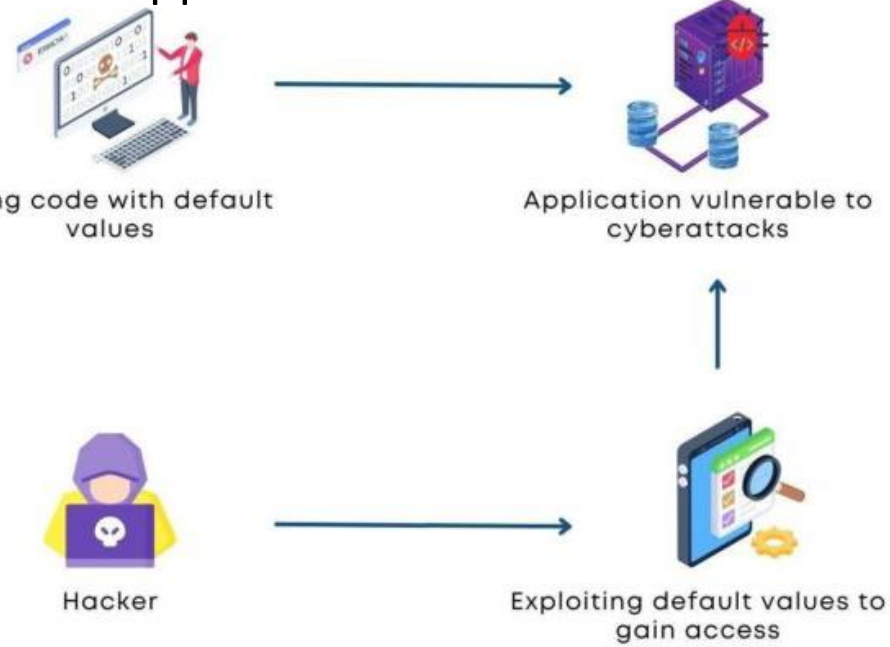
Дефиниране на проблемите

ТИПОВЕ АТАКИ

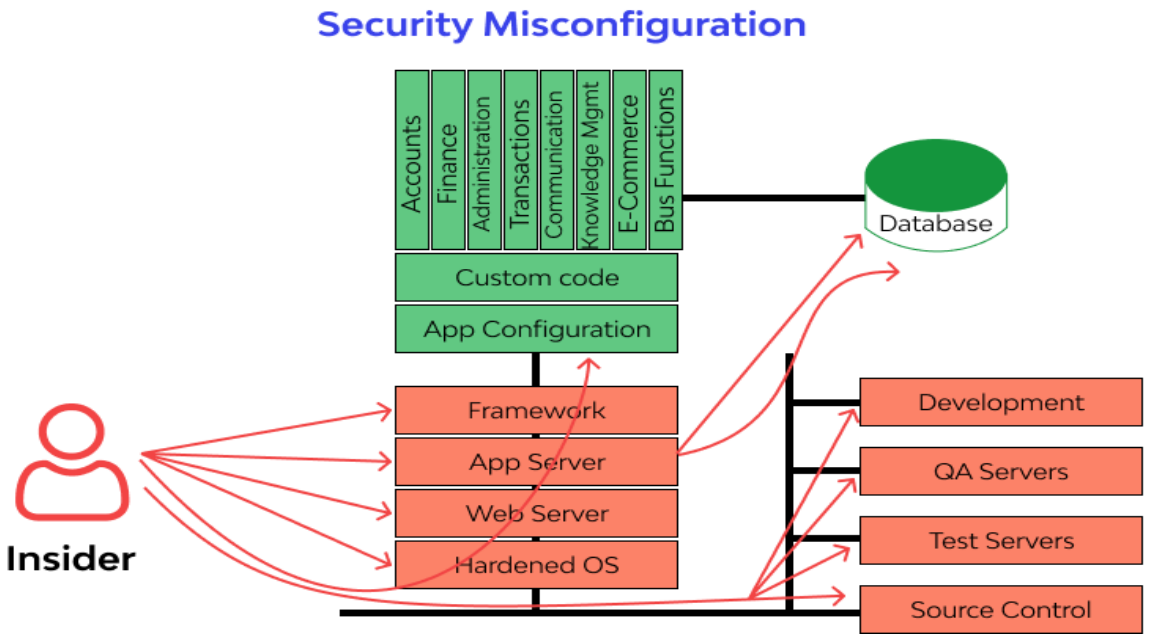


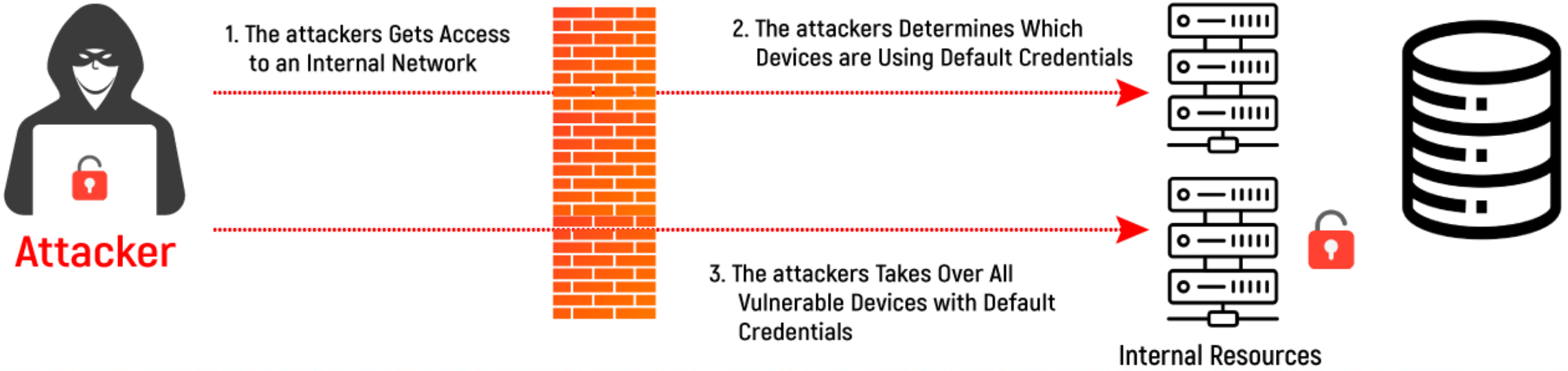
1. Конфигурации по подразбиране на софтуер и приложения
2. Неправилно разделяне на привилегиите на потребителите/администраторите
3. Недостатъчно наблюдение на вътрешната мрежа
4. Липса на мрежова сегментация
5. Лошо управление на ъпдейтите





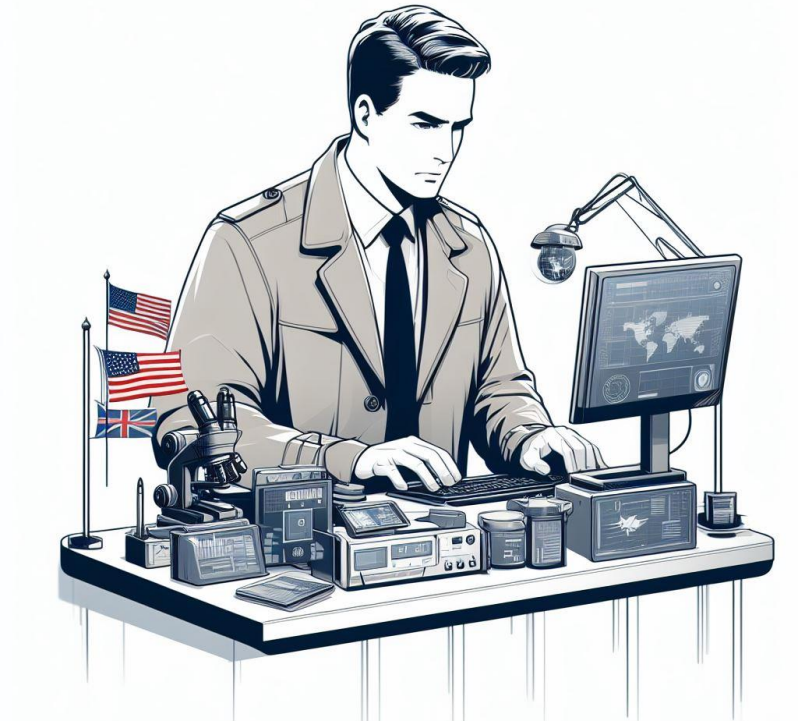
6. Заобикаляне на контрола за достъп до системата
7. Слаби или неправилно конфигурирани методи за многофакторно удостоверяване (MFA)
8. Недостатъчни списъци за контрол на дос (ACL) на мрежови споделяния и услуги
9. Лоша киберхигиена на удостоверенията
10. Неограничено изпълнение на код





Ограничаване на проблемите

Когато една държава изостава в научните постижения и не разполага с капацитет да постигне сравними резултати, тя прибягва до неконвенционални методи, включително промишлен шпионаж и вътрешни атаки.



Агентите, участващи в тези операции, са в постоянна опасност и най-малката грешка може да доведе до тяхното излагане на риск. Ситуацията обаче се промени с цифровизацията на научния сектор.

UK EDITION

SUBSCRIBE: £20 FOR 1 YEAR | LOG IN / REGISTER

INDEPENDENT

Rugby World Cup | Visit The USA | ENHANCED BY Google

NEWS SPORT VOICES CULTURE LIFESTYLE TRAVEL PREMIUM MORE INDEPENDENT tv

News > World > Europe

Russian spy 'stole Oxford/AstraZeneca vaccine blueprint and used it to develop Sputnik jab'

UK security services have allegedly told ministers they now have solid proof an agent stole vital information

Chiara Giordano • Monday 11 October 2021 15:33 BST • Comments

Powered by PIXELS·AI

tv

Asia Australia Middle East Africa Inequality Global development

This article is more than 3 years old

China theft of technology is biggest law enforcement threat to US, FBI says

- Christopher Wray says China using 'any means necessary'
- Chinese theft of US trade secrets costing '$300bn-$600bn a year'

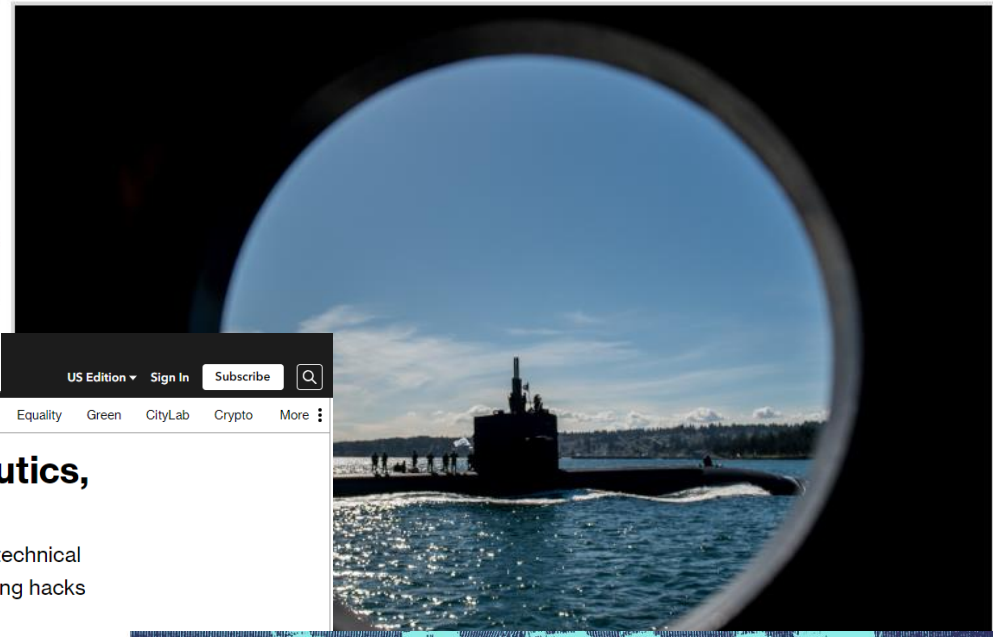
A lamp post outside the White House is adorned with Chinese and US national flags in Washington. Photograph: Jewel Samad/AFP via Getty Images

The FBI on Thursday identified China as the biggest law enforcement threat to the United States, and its director said Beijing was seeking to steal

China Has Stolen Vast Amounts of Navy Submarine, Missile Data in Multiple Breaches from Contractor's Servers

By: Sam LaGrone

June 8, 2018 4:26 PM • Updated: June 8, 2018 7:09 PM



US Edition | Sign In | Subscribe

dustries Tech AI Politics Wealth Pursuits Opinion Businessweek Equality Green CityLab Crypto More

SECURITY / POLICY / TECH

23andMe says it's looking into another possible data leak

/ The hacker tha
the last 23andM
they've obtained
genetic informati

By Emma Roth, a news writer who covers crypto, social media, and much more. Pre MUO.

Oct 19, 2023, 6:49 PM GMT+3 | 6 C

Photo by Amelia Holowaty Krales / The Verge

23andMe is investigating reports of a new data leak involving millions of user records. On Wednesday, *TechCrunch* reported that a hacker claims to have leaked 4 million genetic profiles belonging to people in Great Britain, along with "the wealthiest people living in the U.S. and Western Europe."

The hacker, who goes by "Golem," is the same one that stole 1 million

1 Fr cla riv

2 So

3 Mi

Technology
Cybersecurity

Gift this article

China Says US Hacked Aeronautics, Space Research University

- NSA is accused of cyberattacks on Northwestern Polytechnical
- China has been more direct in accusing US of conducting hacks

By Sarah Zheng

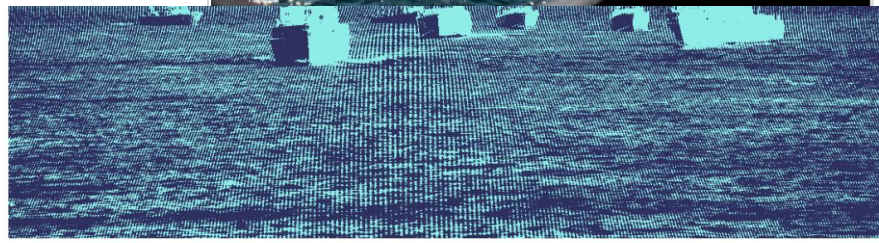
September 5, 2022 at 7:15 AM GMT+3
Updated on September 6, 2022 at 2:19 AM GMT+3

Save

This article is for **subscribers only**.

China accused a US spy agency of hacking a government-funded university with aeronautics and space research programs, in Beijing's latest effort to hit back at Washington's complaints of cybersnooping.

The National Security Agency's Office of Tailored Access Operations carried out the attacks on Northwestern Polytechnical University in Xi'an, China's National Computer Virus Emergency Response Center said in a statement. A team from the center and 360 Security Technology Inc. analyzed the university's information systems after an attack from overseas was reported in June, the center added.



NAVY-ARMY|CISA-FIGURE

Catalin Cimpanu
February 16th, 2022

Government
Nation-state News

US says Russian hackers breached multiple DOD contractors

The US government said today that Russian state-sponsored threat actors have targeted and breached multiple defense contractors between January 2020 and February 2022.

"Compromised entities have included CDCs [cleared defense contractors] supporting the US Army, US Air Force, US Navy, US Space Force, and DoD and Intelligence programs," US

Satellite hack on eve of Ukraine war was a coordinated, multi-pronged assault

The satellite hack that took the world by storm was more complex than initially thought, according to a Viasat executive.

BY CHRISTIAN VASQUEZ AND ELIAS GROLL • AUGUST 10, 2023

Threat Briefing

Briefing 2: Hackers Target ALMA Observatory with Cyber Attack

By: Joel Francis, Space ISAC – November 15, 2022

Tweet | Share | Share | E-mail

News > Tech

Hackers shut down 2 of the world's most advanced telescopes

By Brett Tingley published August 30, 2023

It's unclear exactly what the nature of the cyberattacks from where they originated.

Comments (12)

Gemini North, located on Maunakea in Hawaii. Gemini North is one half of the Internatio Observatory, a Program of National Science Foundation's NOIRLab. (Image credit: Intern Observatory/NOIRLab/NSF/AURA/P. Horálek (Institute of Physics in Opava))

Some of the world's leading astronomical observatories have repo

Satellite Turla: APT Command and Control in the Sk

APT REPORTS 09 SEP 2015 9 minute read

// AUTHORS

STEFAN TANASE

How the Turla operators hijack satellite Internet links

Have you ever watched satellite television? Were you amazed by the diversity of TV channels and radio stations available? Have you ever looked in wonder at satellite phones or satellite-based Internet connections wondering what makes them tick? What if we told you that there's more to satellite-based Internet connections than entertainment, traffic and weather? Much, much more.

SAFEGUARDING THE US SPACE INDUSTRY

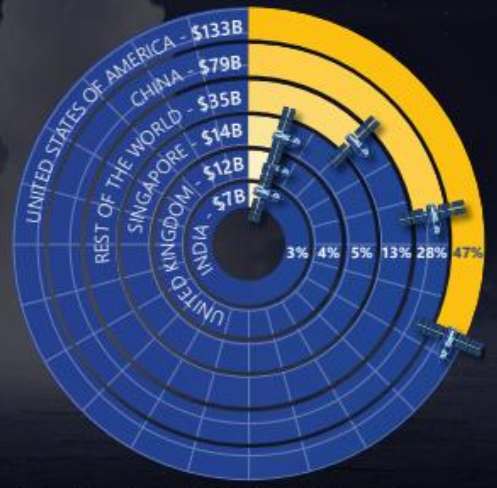
KEEPING YOUR INTELLECTUAL PROPERTY IN ORBIT

THREAT

According to US financial sector estimates, the global space economy is projected to grow from $469 billion in 2021 to more than $1 trillion by 2030. The United States is the main driver of this growth through its role as a global leader in space investment, research, innovation, and production. Space is fundamental to every aspect of our society, including emergency services, energy, financial services, telecommunications, transportation, and food and agriculture. All rely on space services to operate.

Foreign intelligence entities (FIEs) recognize the importance of the commercial space industry to the US economy and national security, including the growing dependence of critical infrastructure on space-based assets. They see US space-related innovation and assets as potential threats as well as valuable opportunities to acquire vital technologies and expertise. FIEs use cyberattacks, strategic investment (including joint ventures and acquisitions), the targeting of key supply chain nodes, and other techniques to gain access to the US space industry.

SPACE EQUITY INVESTMENT 2013-2023 (Q2)



Source: https//www.spacecapital.com/quarterly

IMPACT

FIE efforts to target and exploit the US space industry can harm US commercial firms and broader US national and economic security in several ways.

Global Competition

- Siphoning intellectual property and other proprietary data from US space firms for the benefit of foreign powers' national security programs.
- Leapfrogging innovation that costs US space firms substantial time and resources to generate.
- Using state-backed resources and unfair business practices to disadvantage US space firms.
- Harming US corporate reputations by proliferating counterfeit products or falsely authenticated reproductions.

National Security

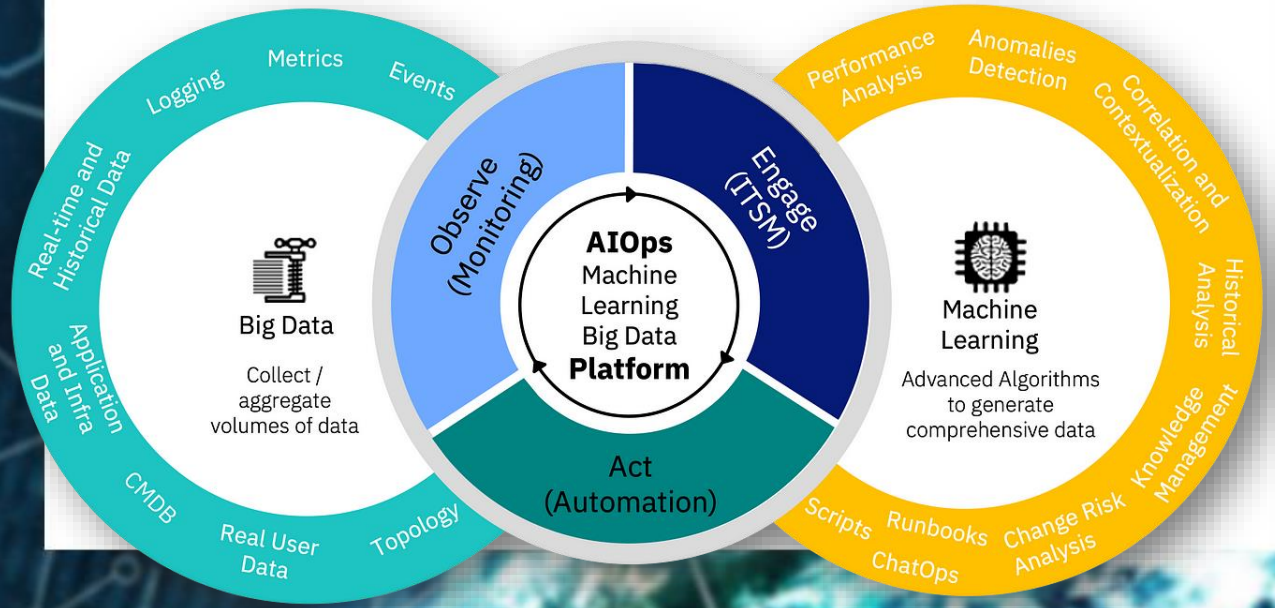
- Collecting sensitive data related to satellite payloads.
- Disrupting and degrading US satellite communications, remote sensing, and imaging capabilities.
- Degrading the United States' ability to provide critical services during emergencies.
- Identifying vulnerabilities and targeting US commercial space infrastructure during conflict.

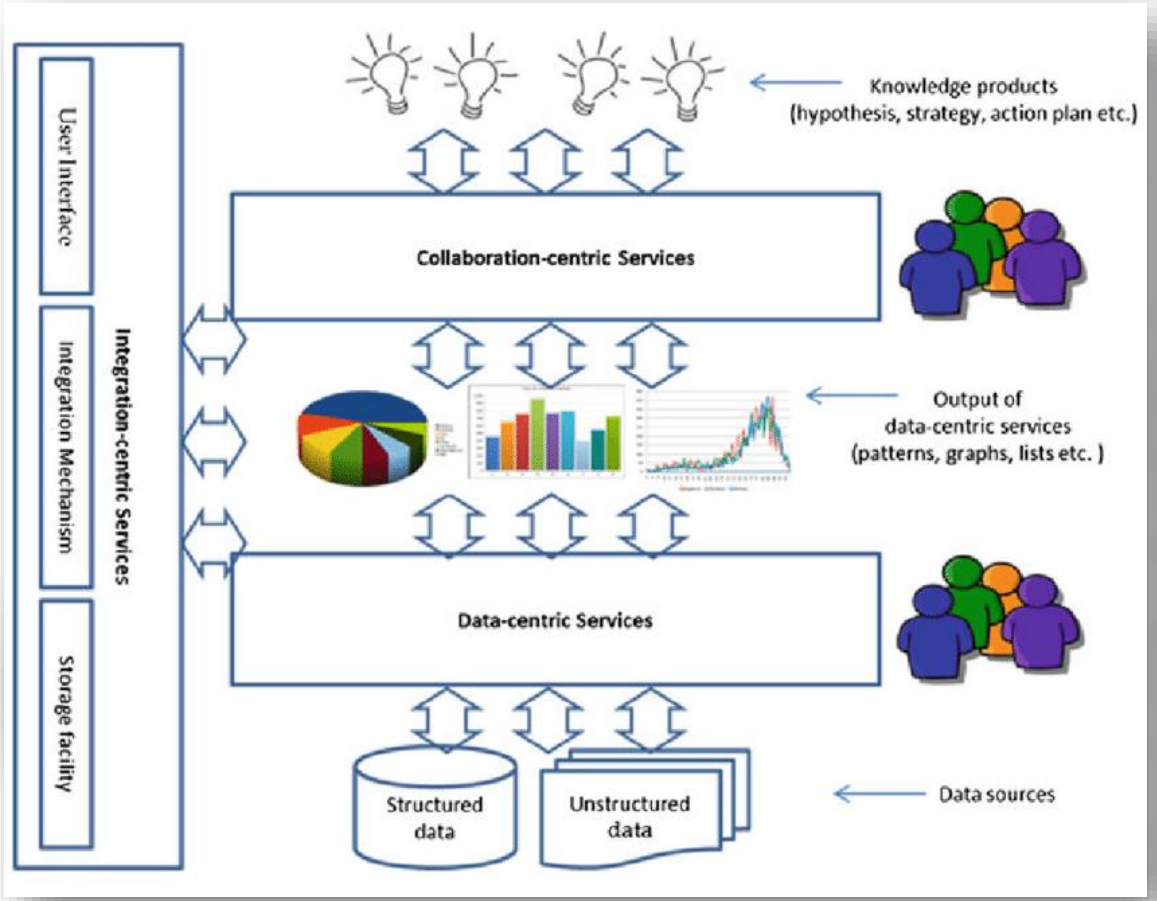
Economic Security

- Harming the US commercial space sector by causing losses of revenue and global market competitiveness.
- Exploiting critical resources and supply chain dependencies.
- Influencing international laws, norms, and host country business regulations governing space to disadvantage US space firms.

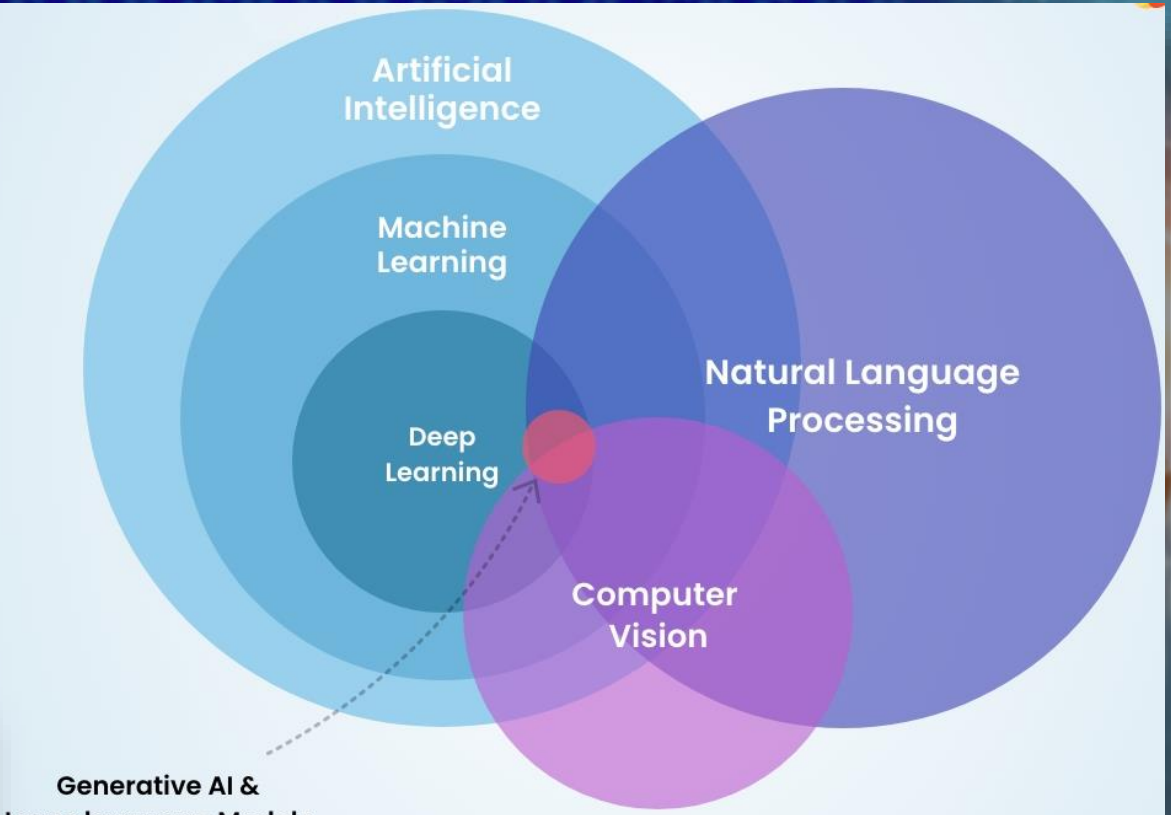
РОЛЯТА НА ГОЛЕМИТЕ ЕЗИКОВИ МОДЕЛИ И ГОЛЕМИТЕ ДАННИ

Големите езикови модели са усъвършенствани системи за изкуствен интелект, които се обучават върху големи обеми от текстови данни, за да разбират моделите и връзките между думи и фрази.





LLM имат широк спектър от приложения и помагат за решаването на някои от най-сложните проблеми в света. Те могат да разчитат, пишат, кодират и изчисляват, подобрявайки човешката креативност и продуктивност в различни индустрии.



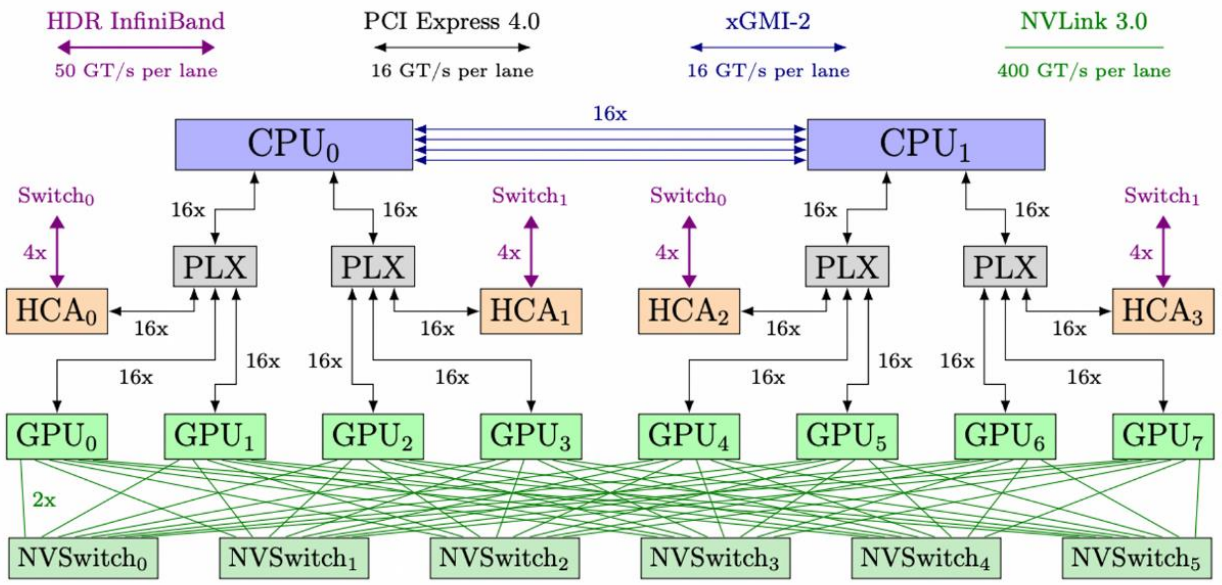
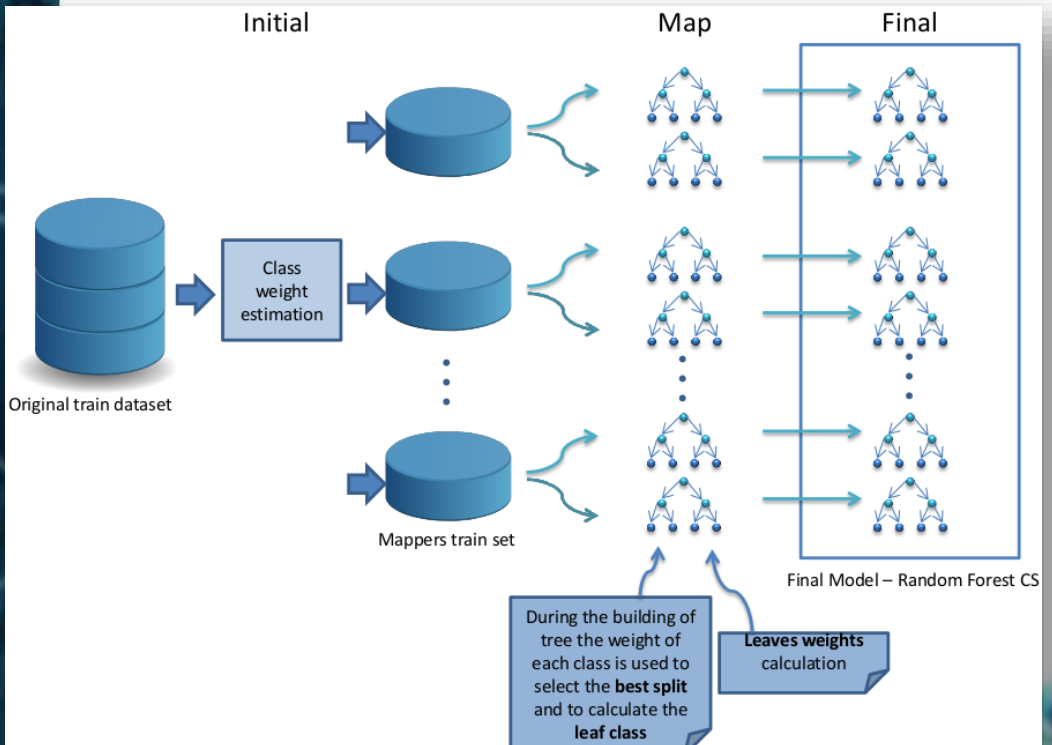
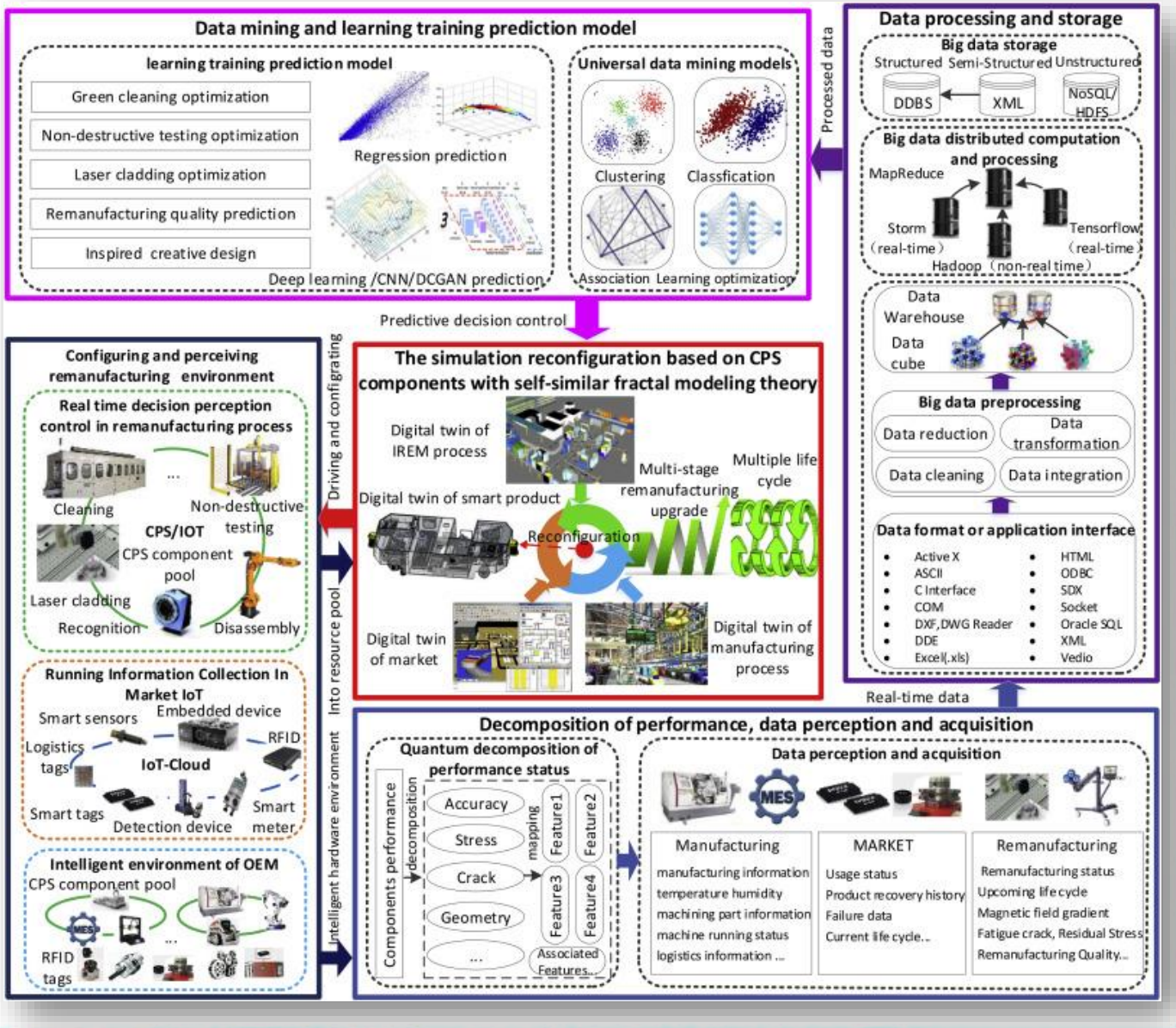


Figure 2: Architecture diagram of a single training node.

Big data, от друга страна, се отнася до изключително големи масиви от данни, които могат да бъдат анализирани изчислително, за да се разкрият модели, тенденции и асоциации.

Големите данни обикновено се характеризират със своя обем, скорост и разнообразие.

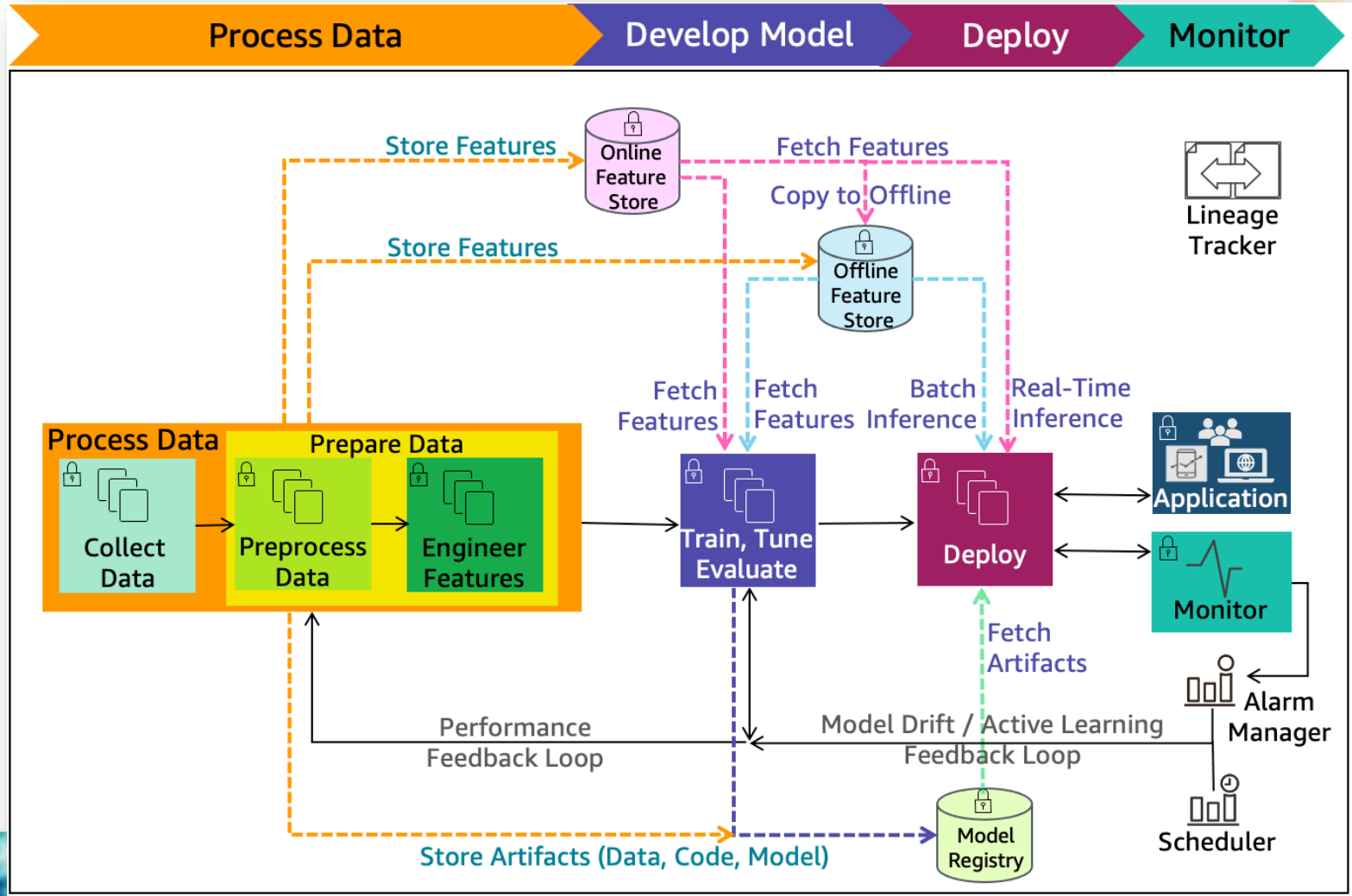




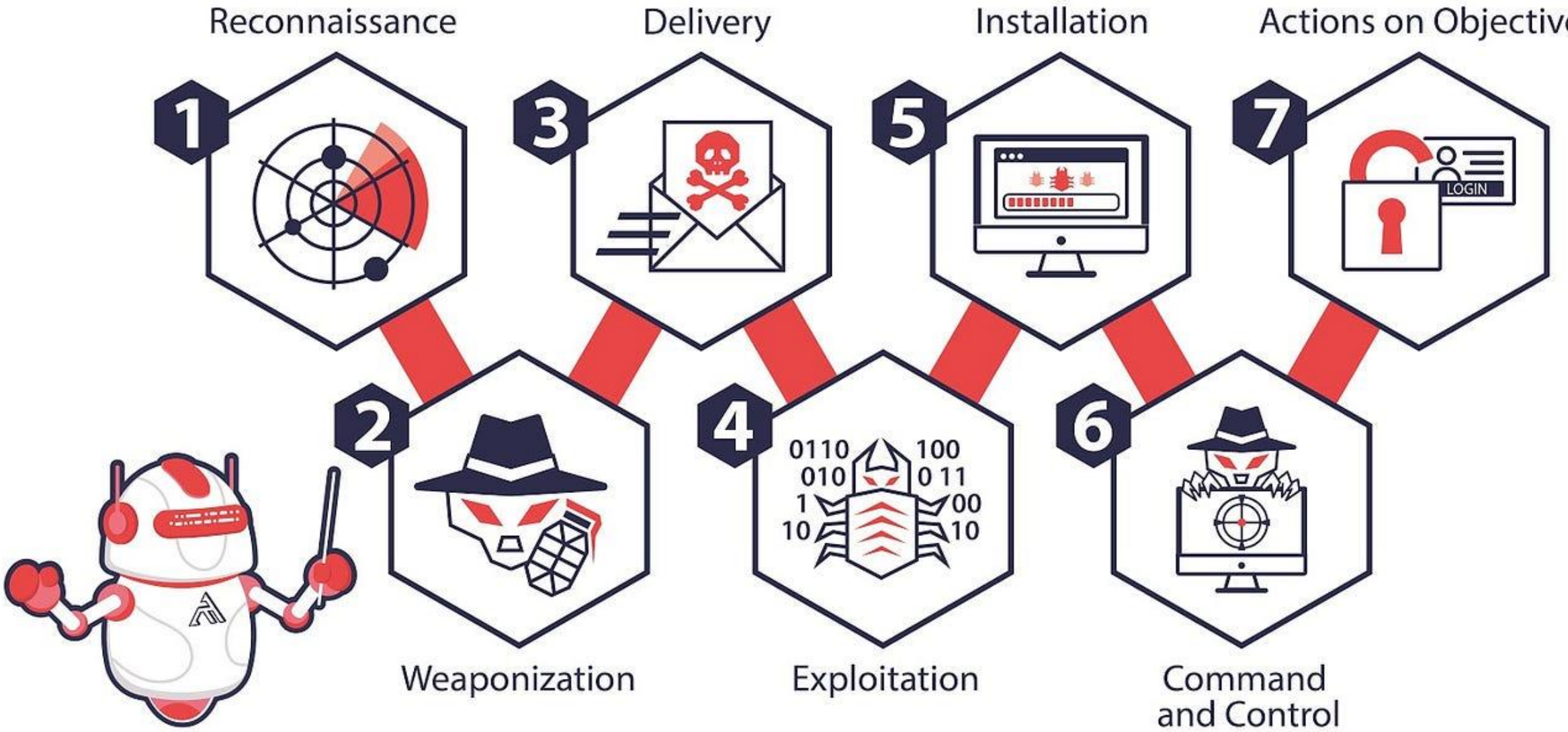
Изкуствения интелект и Cyber kill chain.
Основи на офанзивните възможности като начин за защита.

Стъпките за разработване на кибератаки и зловреден софтуер следват модела Cyber Kill Chain, създаден от Lockheed Martin.

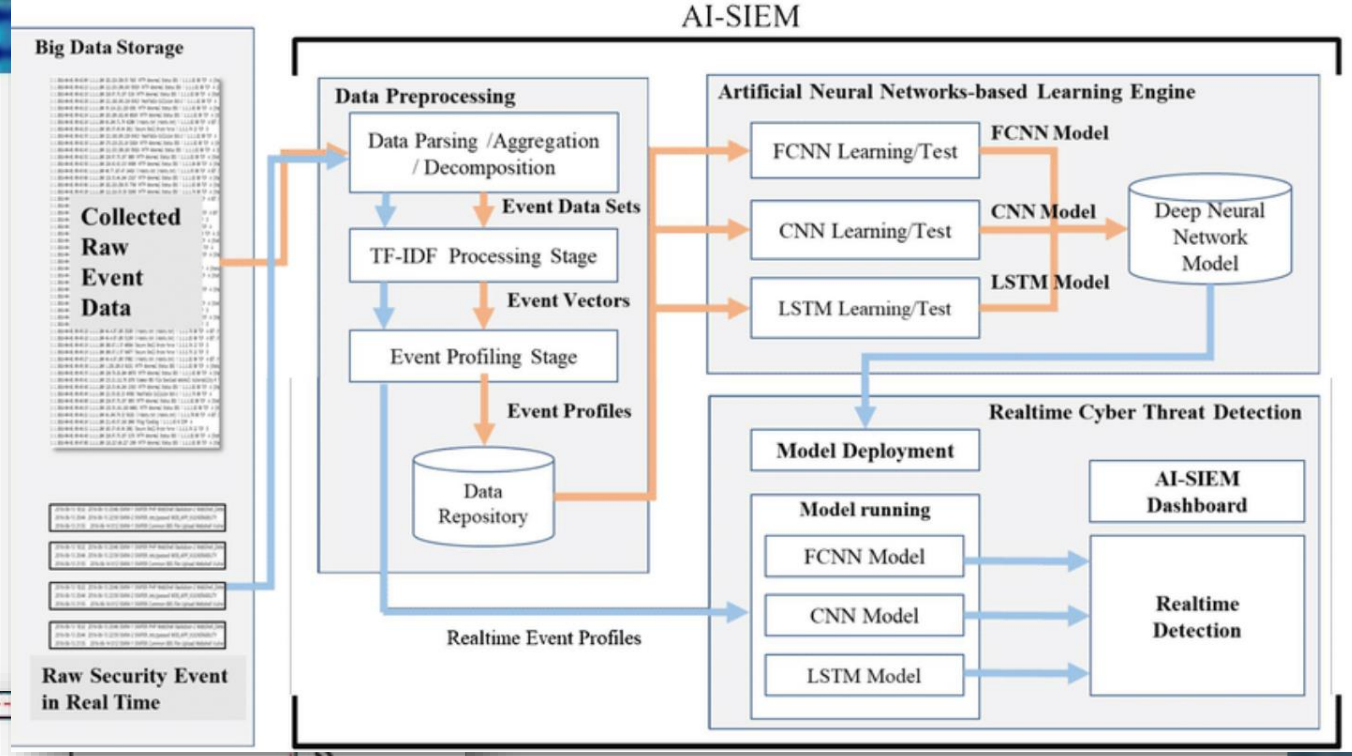
Основните стъпки в тяхното развитие се състоят от разузнаване, милитаризиране на информацията, доставка и експлоатация, инсталиране, командване и контрол и атака над самата цел.

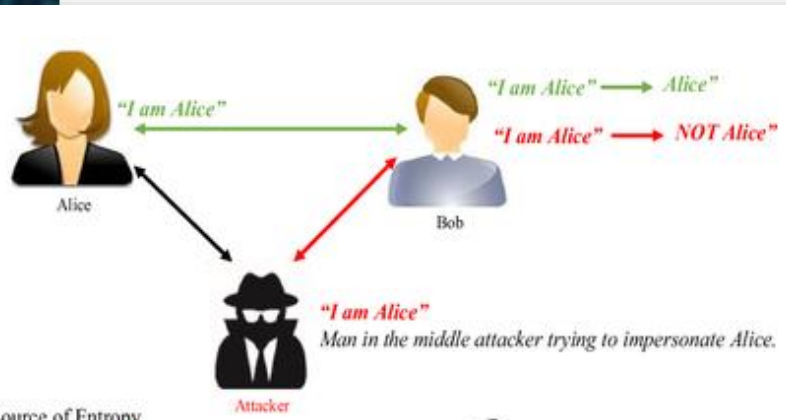


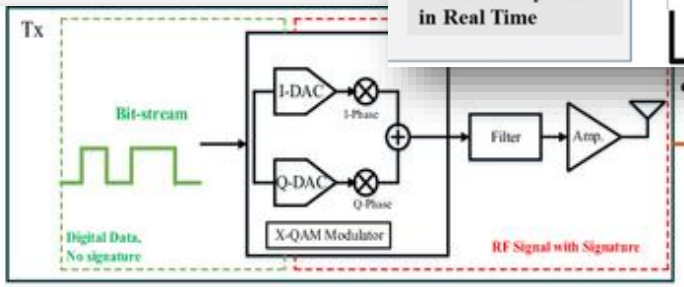
THE CYBER KILL CHAIN

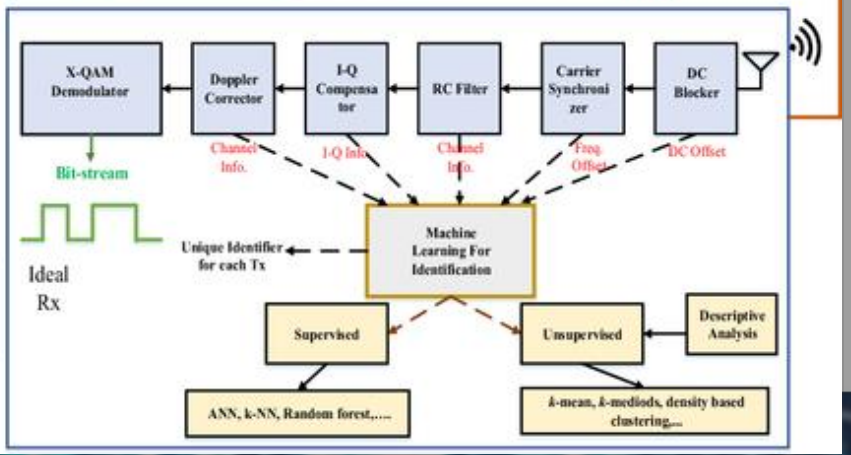


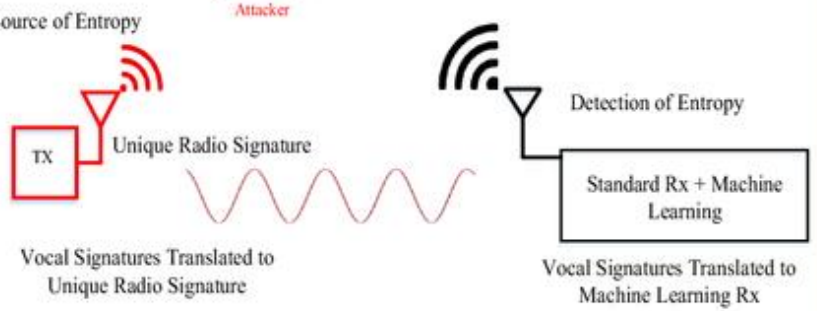
Чрез включването на възможностите на ИИ във всеки етап от веригата Cyber Kill Chain нападателите могат да разработват по-сложни и целенасочени атаки, а защитниците могат да подобрят своите възможности за откриване и реагиране, за да изпреварят възникващите заплахи.







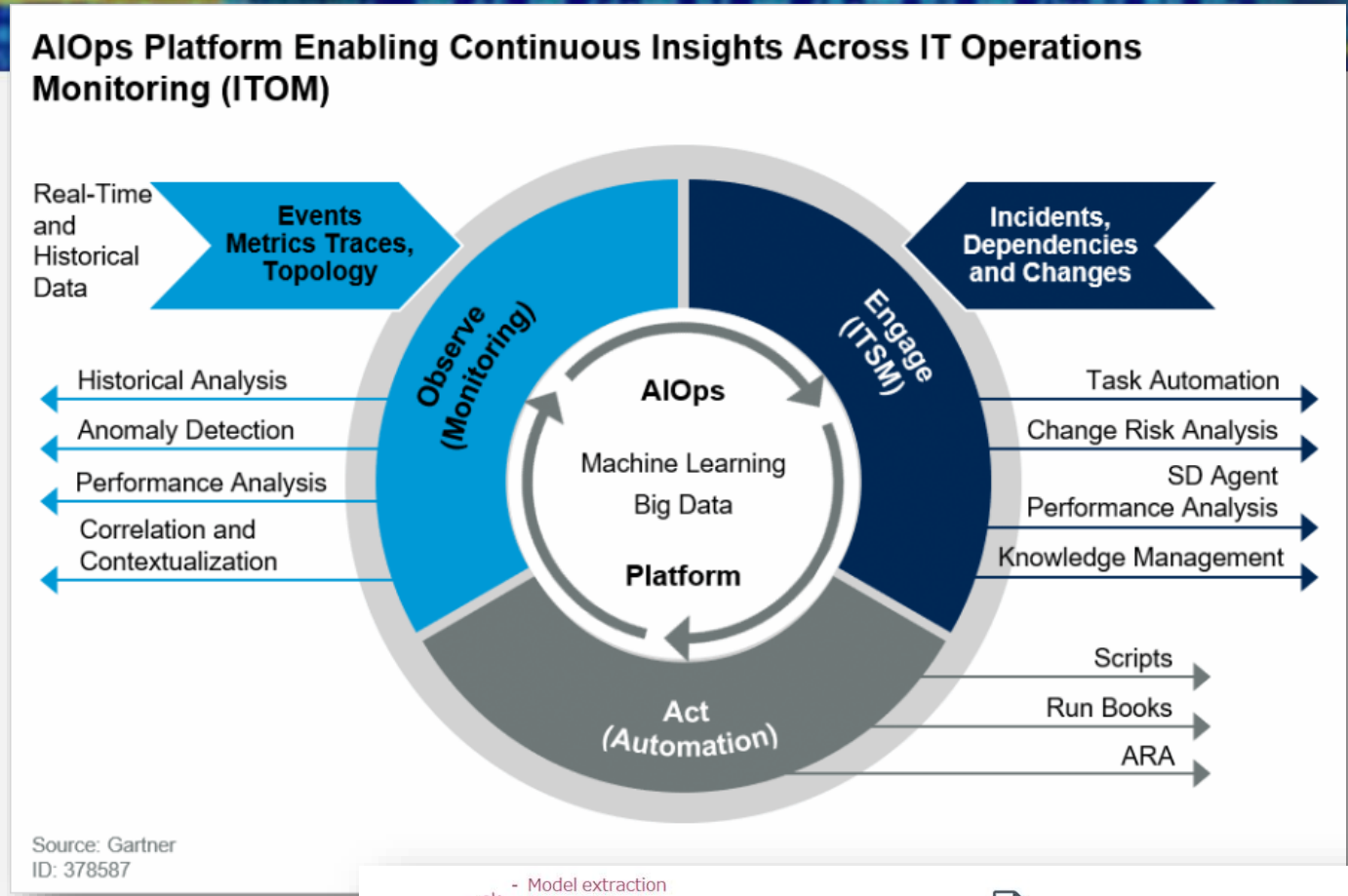


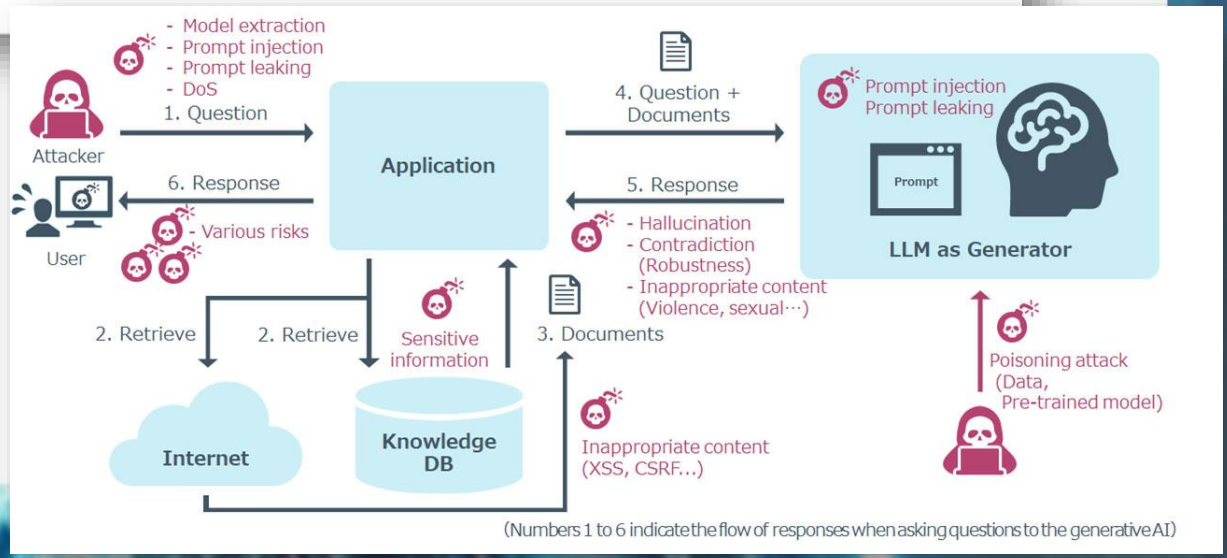


В офанзивен план ИИ може да се използва за автоматизиране на кибератаките, което ги прави по-бързи и по-ефективни.

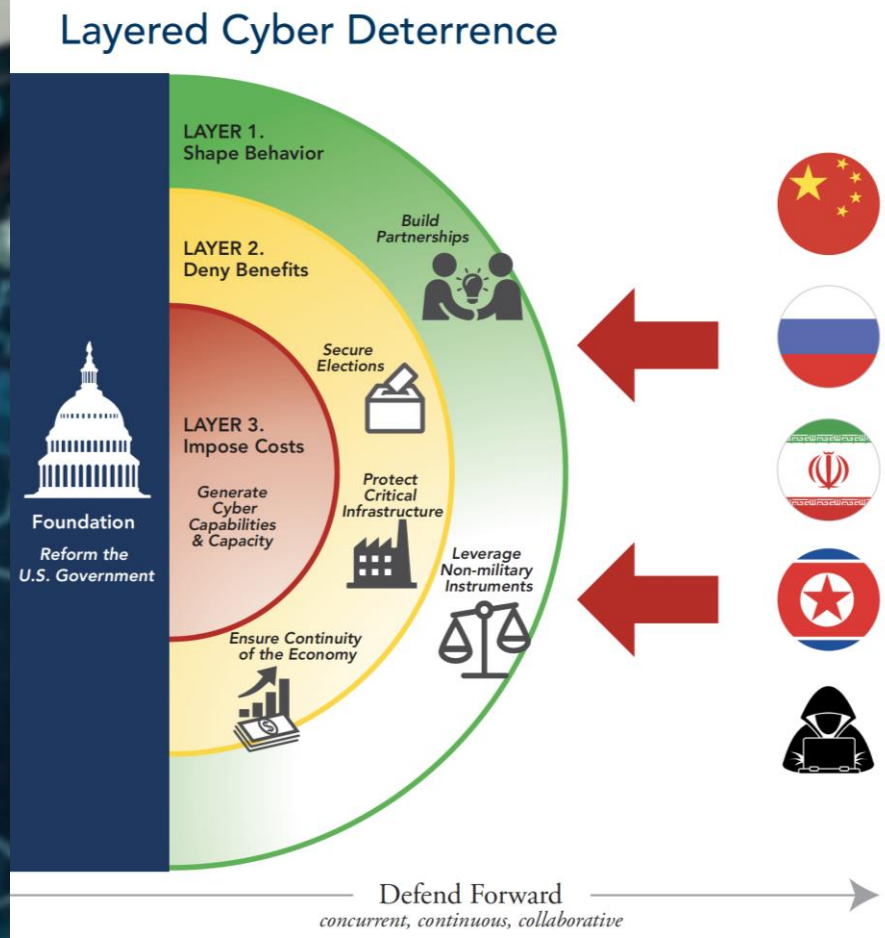
Той може да се използва и за идентифициране на уязвимости в целевите системи и за разработване на нови методи за атака.

От страна на отбраната ИИ може да се използва за откриване и реагиране на киберзаплахи в реално време, като по този начин се подобрява скоростта и ефективността на киберзащитата.





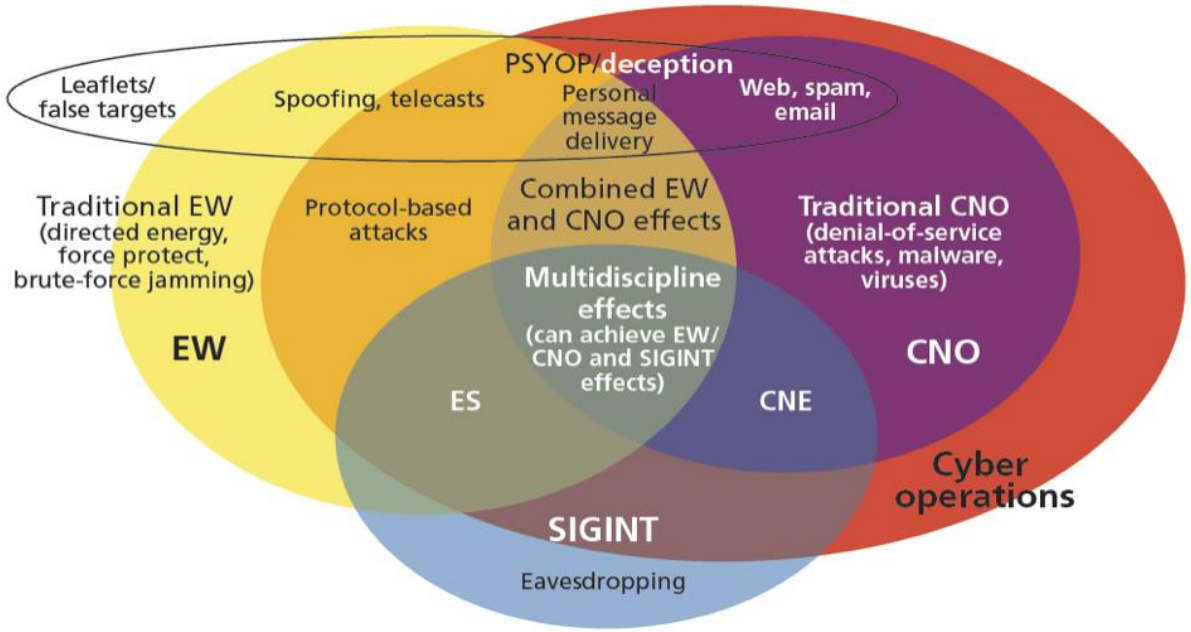
U.S. CYBER STRATEGY 2018

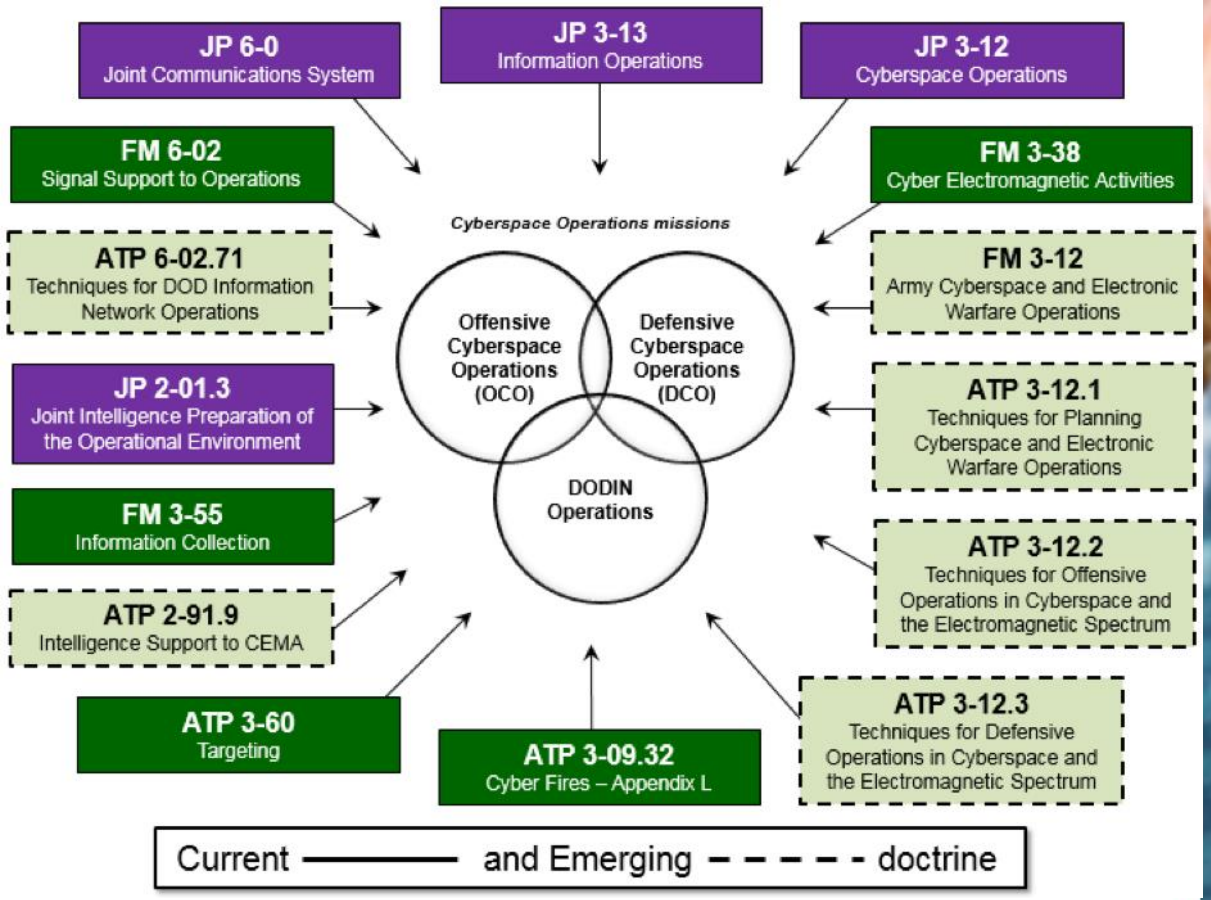


Тази стратегия предостави по-големи правомощия на киберкомандването и подчерта ключови принципи като **defend forward,**
persistent engagement
and proactive deterrence

Този подход надхвърли фокуса, който беше насочен единствено към .gov и .mil, и обхвана по-широка перспектива - граждански мрежи, критична инфраструктура, системи на трети страни и всичко, свързано с нормалното функциониране на страната.

Офанзивните действия срещу противниците са стратегически насочени към разрушаване или саботиране на инфраструктурата, която противниците използват, за да атакуват Съединените щати.

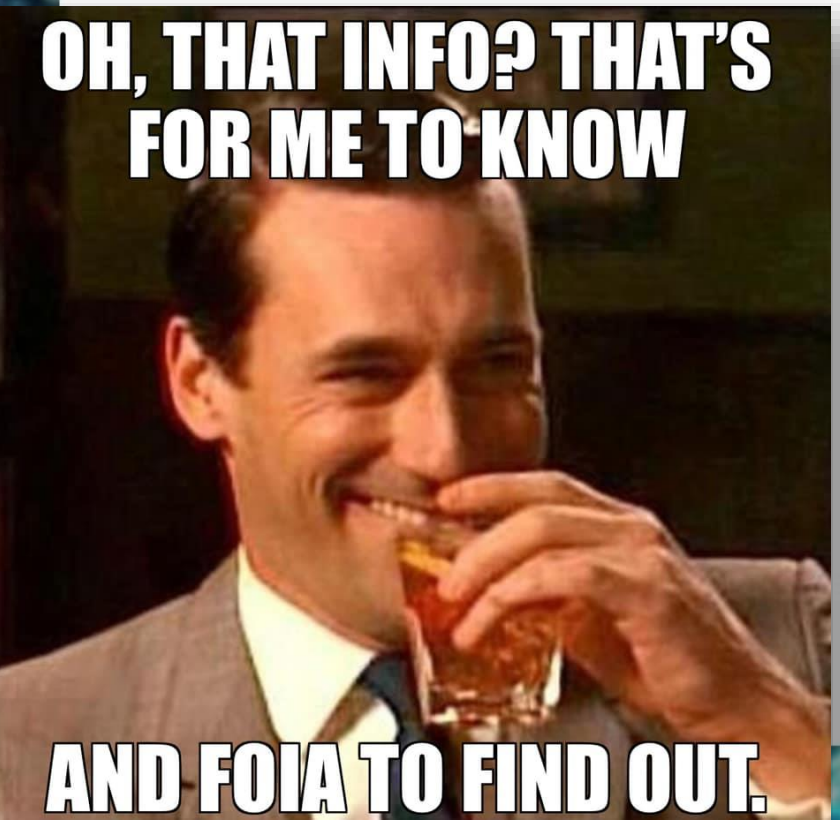


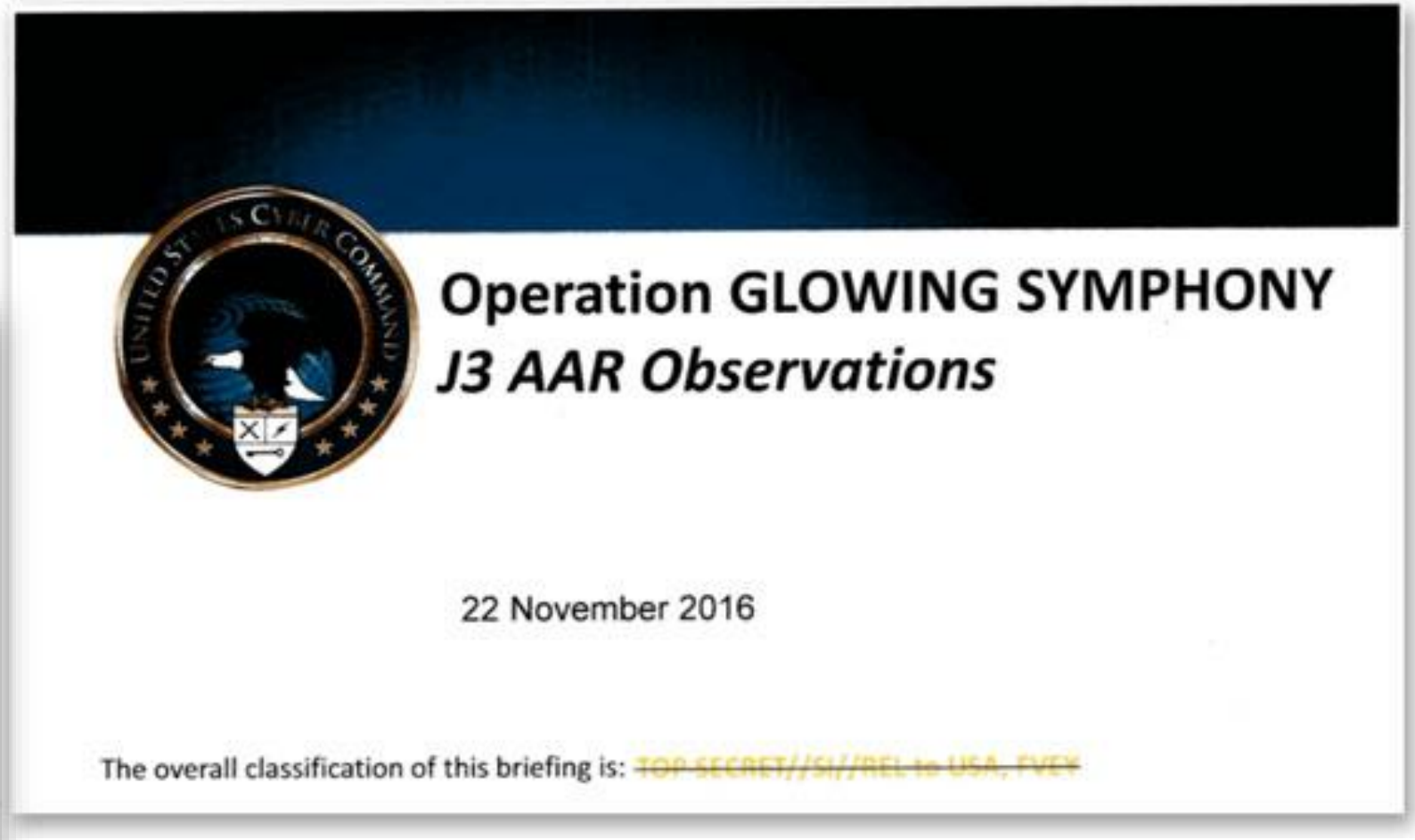


ОПЕРАЦИЯ СИЯЙНА СИМФОНИЯ

FREEDOM OF INFORMATION ACT (FOIA)

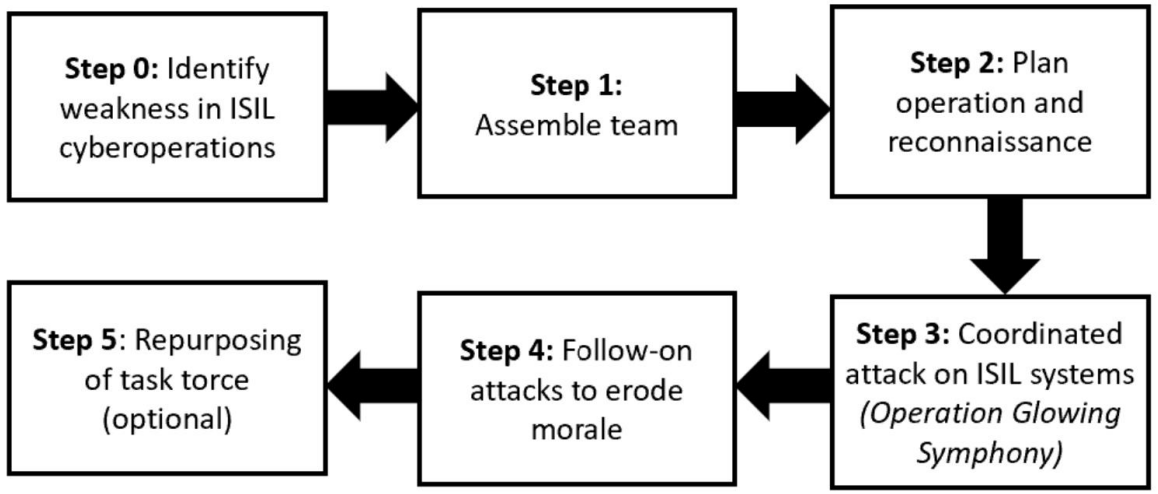
Your right to know

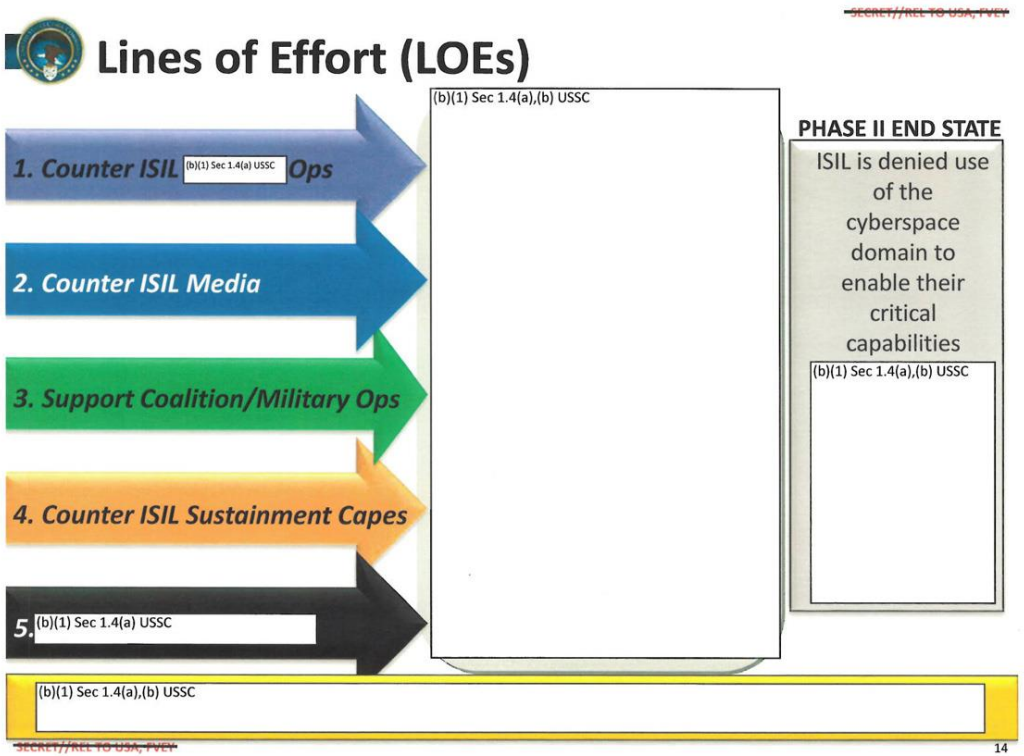




Операция „Сияйна симфония“ послужи като първи прототип за разработване на концепцията за новите операции на САЩ в киберпространството.

Тази операция имаше конкретната цел да разруши напълно медийната пропагандна машина на „Ислямска държава“.





Операция „Сияйна симфония“ беше проведена от Съвместната оперативна група ARES (JTF-ARES), подразделение на Морската пехота на САЩ (MARFORCYEBR)

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre
a part of GCHQ

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

National Cyber Security Centre
PART OF THE GCSB

Hunting Russian Intelligence "Snake" Malware

CYBERSECURITY ADVISORY

DOJ Menu

Office of Public Affairs
U.S. Department of Justice

Our Offices | Find Help | Contact

Search

About | News | Documents | Internships | FOIA | Contact | Information for Journalists

Justice.gov > Office of Public Affairs > News > Press Releases > U.S. Government Disrupts Botnet People's Republic of China Us
To Conceal Hacking of Critical Infrastructure

News

- All News
- Blogs
- Photo Galleries
- Podcasts
- **Press Releases**
- Speeches
- Videos

PRESS RELEASE

U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure

Wednesday, January 31, 2024

Share

For Immediate Release

Office of Public Affairs

Court-Authorized Operation Removed Malware from U.S.-Based Victim Routers and Took Steps to Prevent Reinfection

A December 2023 court-authorized operation has disrupted a botnet of hundreds of U.S.-base
small office/home office (SOHO) routers hijacked by People's Republic of China (PRC) state-

AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

[redacted]

UNITED STATES DISTRICT COURT
for the
Southern District of Texas

United States Courts
Southern District of Texas
FILED
January 09, 2024
Nathan Ochsner, Clerk of Court

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
SPECIFIED ROUTERS IN THE UNITED STATES INFECTED WITH KV BOTNET MALWARE

Case No. **4:24-mc-5018**

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Please see Attachment A of the affidavit, which is attached hereto and made a part of this application.

located in the _____ District of 5+ districts , there is now concealed *(identify the person or describe the property to be seized):*

Please see Attachment B of the affidavit, which is attached hereto and made a part of this application.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more):*

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

TRUE COPY I CERTIFY
ATTEST: January 09, 2024
NATHAN OCHSNER, Clerk of Court
By: [redacted] Deputy Clerk

The search is related to a violation of:

Code Section	*Offense Description*
	18 U.S.C. § 1030(a)(5) (damage to a protected computer) and 371 (conspiracy to commit damage to a protected computer) ("Subject Offenses")

The application is based on these facts:
Please see the attached affidavit, which is attached hereto and made a part of this application.

- ☑ Continued on the attached sheet.
- ☑ Delayed notice of _____ days *(give exact ending date if more than 30 days:* 02/02/2024) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached

[redacted]
Applicant's signature

[redacted]
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by

News

All News

Blogs

Photo Galleries

Podcasts

Press Releases

Speeches

Videos

PRESS RELEASE

Justice Department Conducts Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate of the General Staff (GRU)

Thursday, February 15, 2024

Share

For Immediate Release

Office of Public Affairs

AO 93 (Rev. 12/09) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

IN THE MATTER OF THE SEARCH OF SPECIFIED ROUTERS IN THE UNITED STATES INFECTED WITH MOOBOT MALWARE

Case No. 24-MJ-129

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Pennsylvania and elsewhere:

SEE ATTACHMENT A

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before February 9, 2024 *(not to exceed 14 days)*

☐ In the daytime 6:00 a.m. to 10 p.m. X at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge Richard A. Lloret *(name)*.

X I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized for 30 days.

Date and time issued: 1/26/2024 3:31 pm — */s/ The Honorable Richard A. Lloret* *Judge's signature*

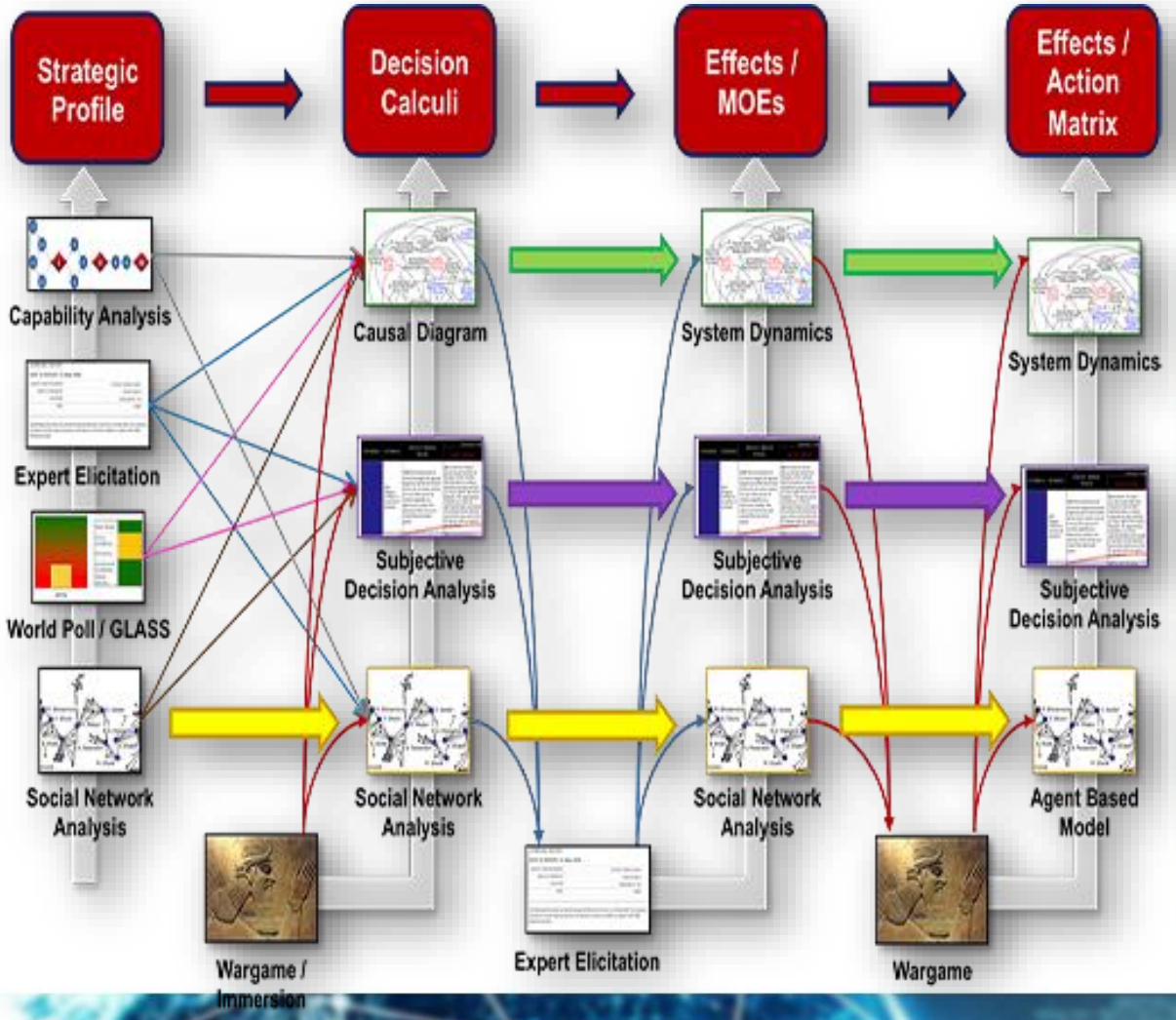
City and state: Philadelphia, PA — HON. RICHARD A. LLORET, USMJ *Printed name and title*

Изкуствения интелект и регулациите в дефанзивните операции

Регулациите могат да имат непредвидени последици, вместо да служат само като защитни механизми.

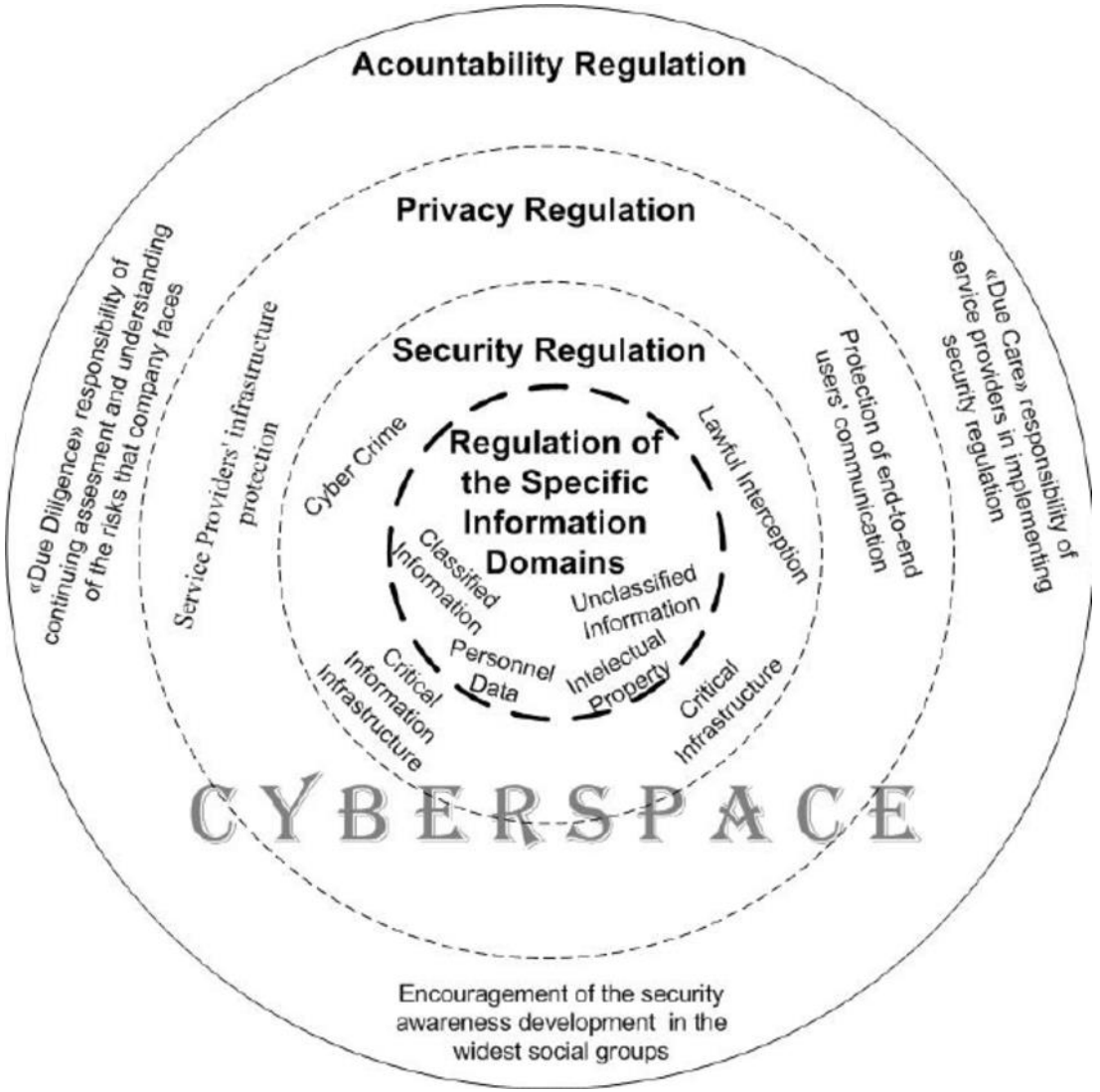
Те могат да въведат усложнения, да натоварят предприятията с изисквания за съответствие и да създадат нови уязвимости в организационните инфраструктури

Неяснотите и променливостта на регулаторната среда представляват значителни предизвикателства за организациите, които се опитват да се адаптират към променящите се изисквания за съответствие.



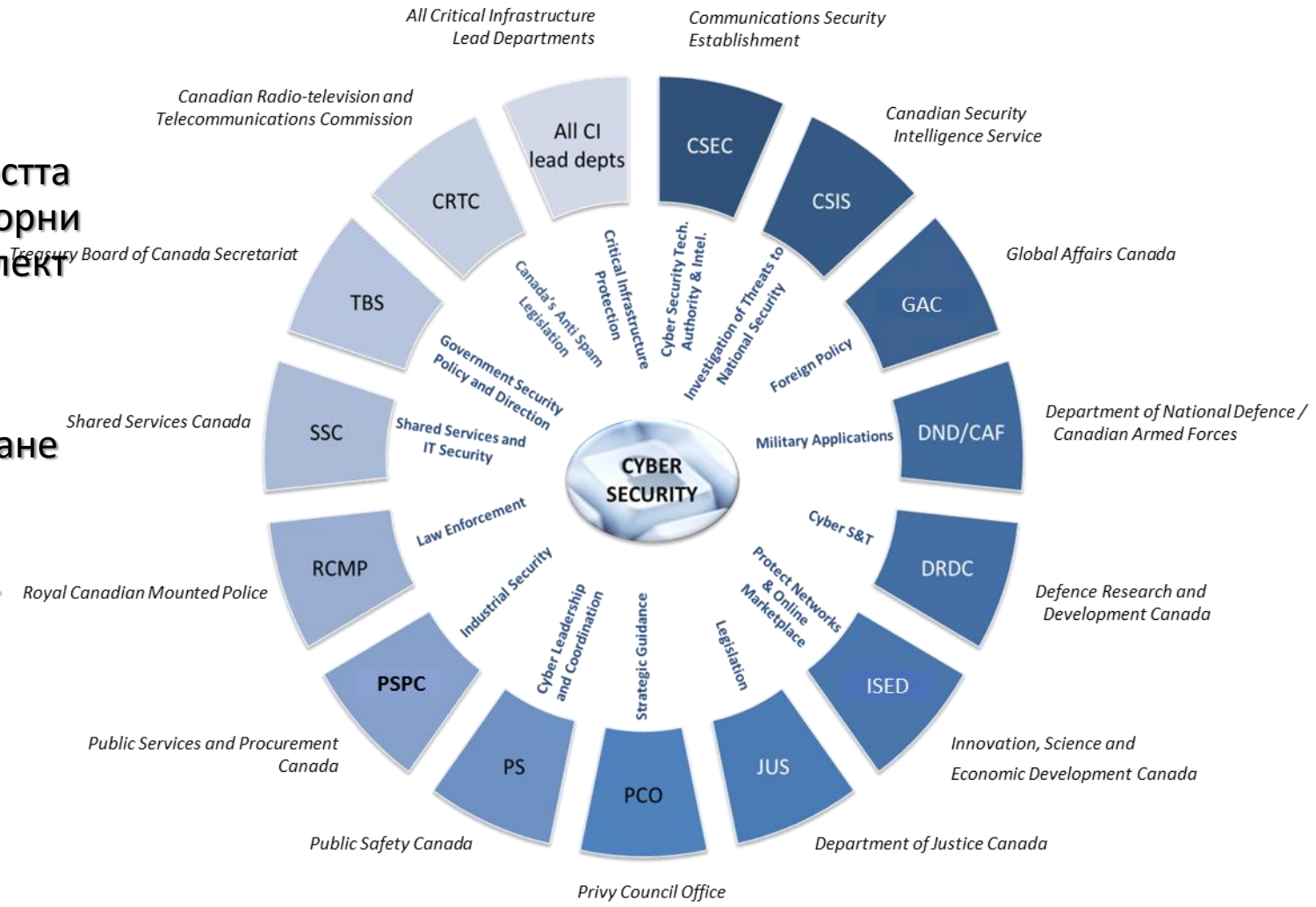
Бързият темп на технологичен напредък в областта на ИИ и кибероперациите изпреварва способността на регулаторните рамки да вървят в крак с него, което води до регулаторни пропуски, оставяйки организациите уязвими за киберзаплахи.

В глобалния контекст на кибероперациите и взаимосвързаността на цифровите системи, необходимостта от по-гъвкава и адаптивна регулаторна рамка става още по-належаща.



дерегулациите подчертават необходимостта от преоценка на традиционните регулаторни подходи в областта на изкуствения интелект и кибероперациите.

Преходът към по-гъвкави и адаптивни стратегии може да помогне за балансиране между сигурността и иновациите, като същевременно адресира сложността и динамичния характер на цифровата ера.



Заключение

В заключение, изследването на приложенията на изкуствения интелект в кибероперациите разкрива многостранен пейзаж, в който технологичният напредък се пресича с регулаторни предизвикателства.

Презентацията подчертава решаващата роля на изкуствения интелект в различните етапи на Cyber Kill Chain, от анализа на уязвимостите до командването и контрола, като подчертава как системите, управлявани от изкуствен интелект, могат да повишат сложността на кибератаките, като същевременно укрепват защитните механизми.