



# **ГЛОБАЛЬНІ ТЕХНОЛОГІЧНІ ТРЕНДИ У СФЕРІ ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ**

Міністерство освіти і науки України  
ДНУ «Український інститут науково-технічної експертизи та інформації»

**Писаренко Тетяна Василівна**

**Кваша Тетяна Костянтинівна**

**ГЛОБАЛЬНІ ТЕХНОЛОГІЧНІ ТРЕНДИ У СФЕРІ  
ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ**

Київ 2020

**УДК 001.18; 002.513.5; 355/359 - 356.252.5**

**ПЗ4**

**ISBN 978-966-479-117-2 (Online)**

**Автори:**

**Писаренко Тетяна Василівна**, заст. директора УкрІНТЕІ

**Кваша Тетяна Костянтинівна**, зав. відділу УкрІНТЕІ

Рекомендовано до друку вченою радою Українського інституту науково-технічної експертизи та інформації МОН України (протокол № 6 від 28.09.2020 р.)

**Рецензенти:**

**Пекарєв Дмитро Володимирович**, кандидат технічних наук, головний науковий співробітник Секції прикладних проблем Президії НАН України.

**Камишин Володимир Вікторович**, доктор пед. наук, канд. техн. наук, с. н. с., член-кор. Національної академії педагогічних наук України, лауреат Державної премії УРСР у галузі науки і техніки та Державної премії України у галузі освіти, директор Українського інституту науково-технічної експертизи та інформації

**ПЗ4 ПИСАРЕНКО Т.В. Глобальні технологічні тренди у сфері озброєння та військової техніки [Електронний ресурс] / Т. Писаренко, Т. Кваша. – К.: УкрІНТЕІ, 2020. – 89 с.**

Викладено результати дослідження щодо глобальних технологічних та наукових трендів у сфері озброєння та військової техніки на основі аналізу публікацій урядів зарубіжних країн, НАТО, SIPRI, Мюнхенської конференції з безпеки, ЄС, міжнародних аналітичних і консалтингових організацій.

Розраховано на представників органів державної влади, експертів, наукових працівників, інженерних кадрів, викладачів закладів вищої освіти.

**УДК 001.18; 002.513.5; 355/359 - 356.252.5**

© МОН України, 2020

© УкрІНТЕІ, 2020

© Писаренко Т.В., Кваша Т.К., 2020

## ЗМІСТ

ВСТУП .....	4
ОГЛЯД ЕКОНОМІЧНИХ ПОКАЗНИКІВ ГЛОБАЛЬНОЇ ВІЙСЬКОВОЇ СФЕРИ.....	5
ОГЛЯД ТЕХНОЛОГІЧНИХ ТРЕНДІВ У ВІЙСЬКОВІЙ СФЕРІ .....	14
ШТУЧНИЙ ІНТЕЛЕКТ.....	19
КІБЕРБЕЗПЕКА І ТЕХНОЛОГІЇ КІБЕРПРОСТОРУ .....	27
АВТОНОМНА ЗБРОЯ ТА РОБОТОТЕХНІКА .....	33
КОСМІЧНІ ТЕХНОЛОГІЇ.....	39
ЯДЕРНА ЗБРОЯ.....	48
ТЕХНОЛОГІЧНА МОДЕРНІЗАЦІЯ ЗБРОЙНИХ СИЛ США.....	55
ВИСНОВКИ.....	65
Додаток А – Бюджет Міністерства оборони на 2021 рік із здійснення військових досліджень і розробок для Повітряних сил США .....	67
СПИСОК ПОСИЛАНЬ .....	84

## ВСТУП

Технологія є фундаментальним фактором соціальних змін, що пропонує нові можливості виробляти, зберігати та поширювати знання. Це особливо стосується військової сфери, основні зрушення в якій часто супроводжуються новаторськими подіями в історії науки та техніки. Якщо спочатку технологія не є результатом військових досліджень та розробок, все одно вона часто знаходить військове застосування і впливає на методи ведення війни. Прогрес у військовій техніці може мати як позитивні, так і негативні наслідки: покращення можливостей запобіжних заходів щодо мобілізації та застосування сили, або більш потужні можливості заподіяння шкоди та знищення.

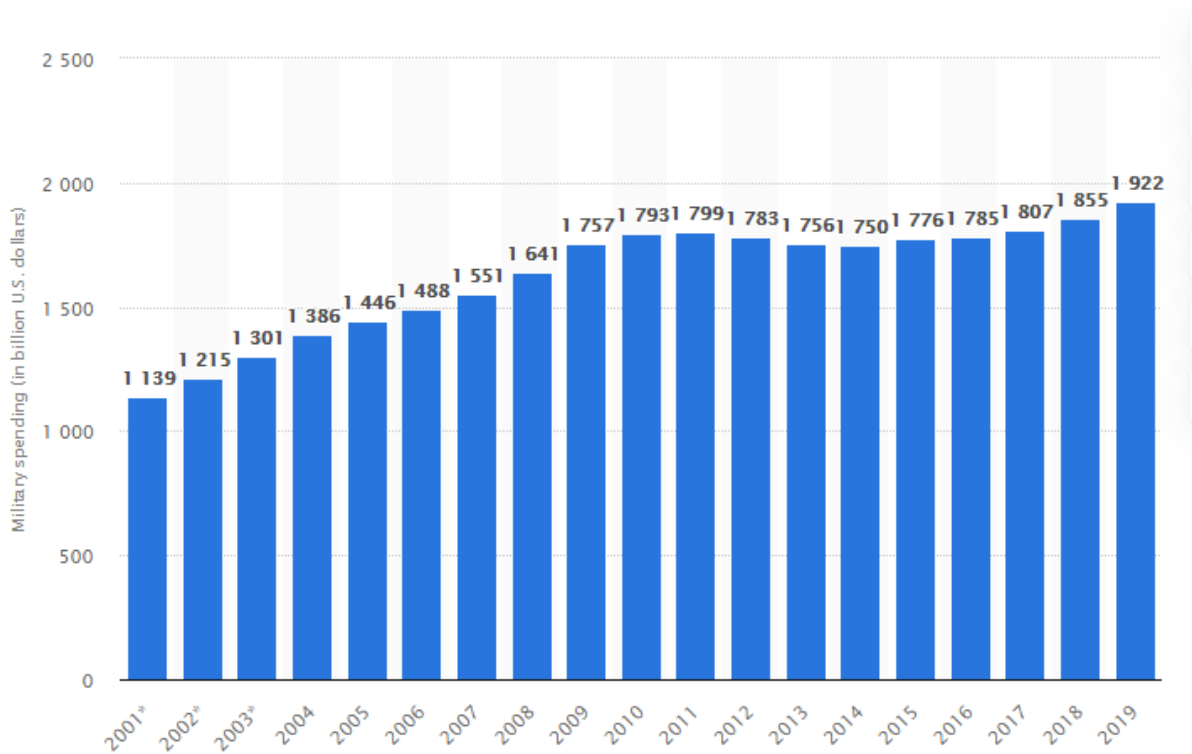
Поточні інновації в галузі штучного інтелекту, робототехніки, автономних систем, космічних технологій, 3D-друку, біотехнології, матеріалознавства та квантових обчислень, як очікується, принесуть безпрецедентні перетворення. За висновками Всесвітнього економічного форуму, вони формують фундамент «четвертої промислової революції». Частково ці технології вже використовуються у військових областях та у сферах безпеки, а частково потребують подальшого вивчення. Штучний інтелект (ШІ) стає "визначальною технологією майбутнього", як у повсякденному житті, так і у військовій сфері.

Щоб розвивати військовий потенціал, придатний для геостратегічних викликів сьогодення та майбутнього, країни повинні залишатися на передовій у галузі інновацій, науки і техніки. Для цього також потрібна оцінка потенційного середовища безпеки у майбутньому, особливо щодо військових викликів та викликів безпеці, що виникають внаслідок нових науково-технічних питань, проривних інновацій.

Моніторинг інновацій і нових технологій є важливим для розуміння майбутніх війн та глобальної безпеки [1]. Дана робота дає представлення про майбутні військові технології за окремими напрямками, що допоможе керівництву армії та країни підготуватися до еволюції майбутнього середовища безпеки та можливих військових дій.

## ОГЛЯД ЕКОНОМІЧНИХ ПОКАЗНИКІВ ГЛОБАЛЬНОЇ ВІЙСЬКОВОЇ СФЕРИ

Світові витрати на оборону у 2019 році склали 1,92 трильйона доларів США, порівняно з 1,14 трильйонами доларів США у 2001 році (у цінах 2018 року) (рис.1). У період 2009 - 2016 рр. витрати стабілізувалися, а з 2017 р. почали зростати знову.

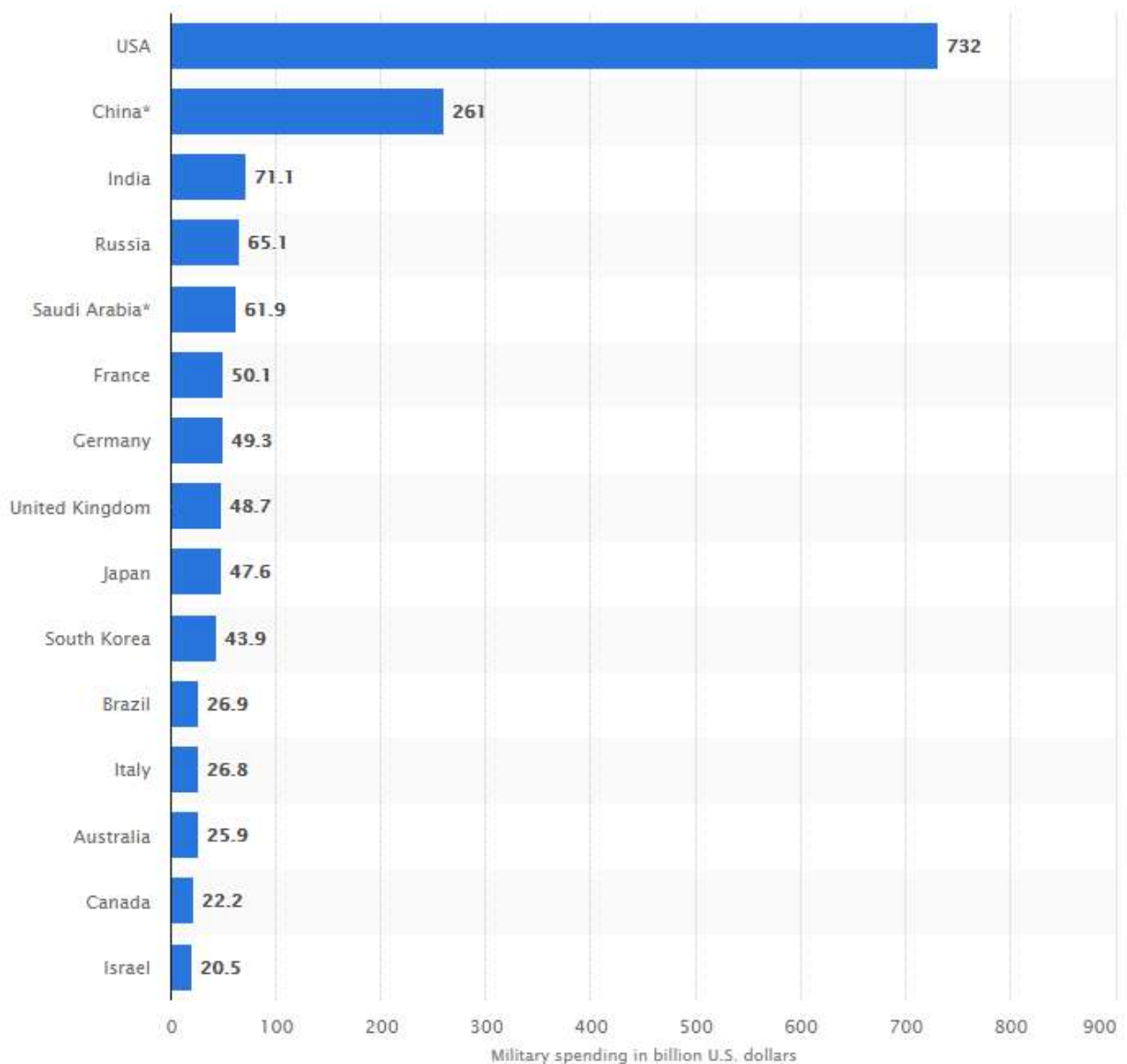


Джерело: Global military spending from 2001 to 2019 (in billion U.S. dollars). - <https://www.statista.com/statistics/264434/trend-of-global-military-spending/>

**Рис. 1** Глобальні військові витрати протягом 2001-2019 рр., млрд дол. США

Найбільший внесок у величезні кошти, витрачених щороку на оборону та озброєння, дають США, які у 2019 р. становили майже 732 мільярда доларів США або 38% глобальних витрат (рис. 2). Китай посів друге місце із 261 млрд дол. США. У період між 2010 і 2019 роками військові витрати Китаю зросли на 85 відсотків.

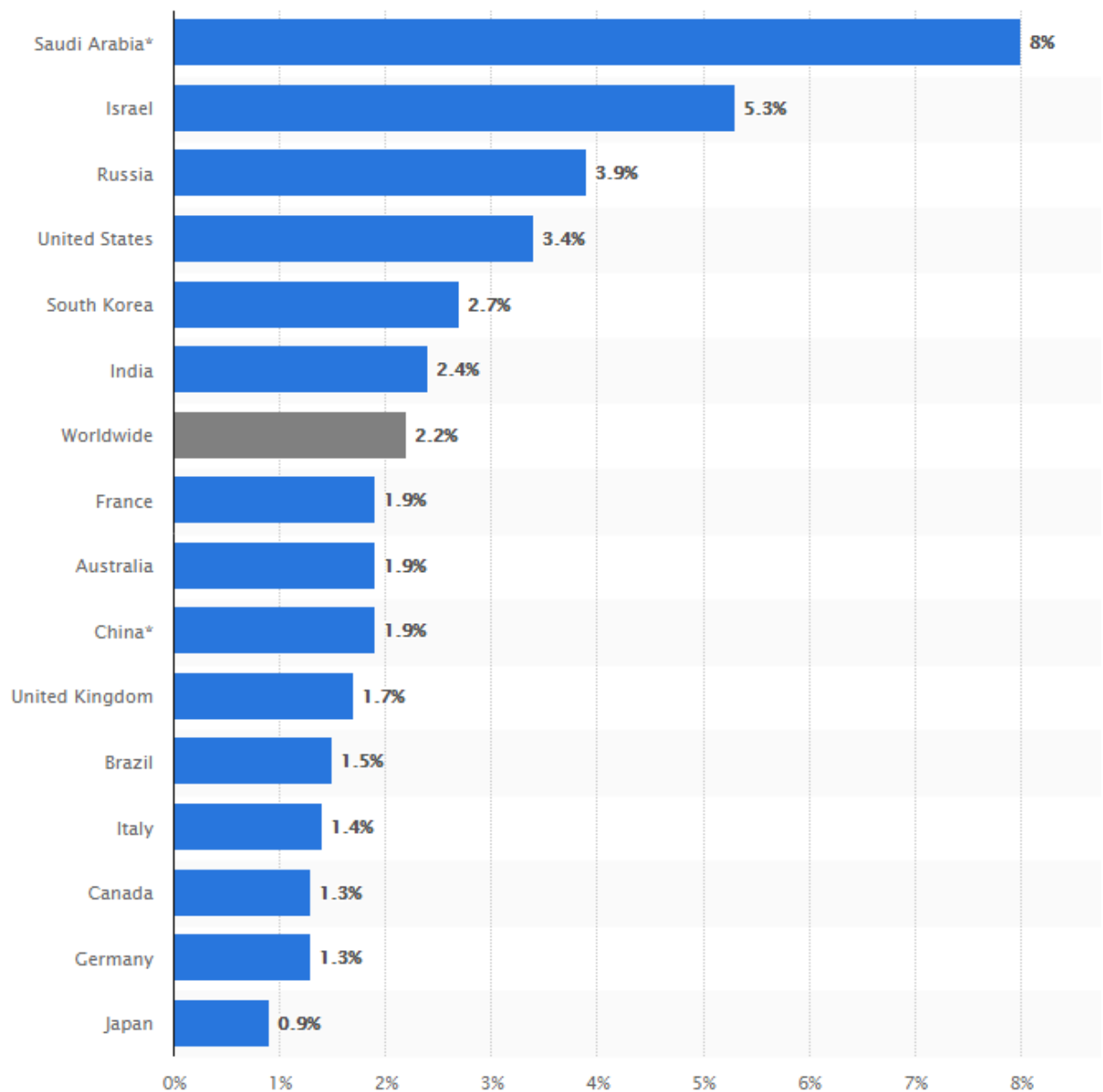
Така велика сума допомогла США зберегти військове домінування у всьому світі, що охоплює низку аспектів, зокрема США володіє більше 25% загальної кількості військових літаків у світі.



Джерело: Military expenditure as percentage of gross domestic product (GDP) in highest spending countries 2019.  
 – Режим доступу: <https://www.statista.com/statistics/266892/military-expenditure-as-percentage-of-gdp-in-highest-spending-countries/>

**Рис. 2 Військові витрати країн із найвищими обсягами витрат у 2019 р., млрд дол. США**

Військові витрати у відсотках до валового внутрішнього продукту є корисним інструментом для оцінки значення, яке окремі держави надають своїм військовим. Цим показником серед усіх інших країн виділяється Саудівська Аравія. У 2019 році 8 відсотків валового внутрішнього продукту країни було витрачено на оборону та озброєння (рис. 3).



**Рис. 3 Військові витрати країн із найвищими витратами у світі, % до ВВП, 2019 рік**

Джерело: Military expenditure as percentage of gross domestic product (GDP) in highest spending countries 2019.  
 – Режим доступу: <https://www.statista.com/statistics/266892/military-expenditure-as-percentage-of-gdp-in-highest-spending-countries/>

Але коли справа стосується військової сили, розмір фінансування, безумовно, має більше значення. Більші країни, такі як США та Китай, мають величезні військові сили, незважаючи на те, що вони витрачають меншу частку свого валового внутрішнього продукту. У Китаї найбільша кількість військових у світі, що становить майже 2,2 мільйона осіб в їхніх лавах. Незважаючи на більший акцент на технології та нове озброєння, чисельність військових у США все ще становить майже 1,3 мільйона.



Defence News<sup>1</sup> у вересні 2020 р. оприлюднило список 100 провідних компаній за обсягами доходів від продажу озброєння та військової техніки. Перші 10 місць займають компанії США, Китаю, Великої Британії (табл. 1). У другій десятці, крім названих, ще компанії з Італії, Франції, Нідерландів і Росії.

**Таблиця 1 - Топ 25 компаній 2020 із виробництва озброєння та військової техніки**

Ранг 2019	Ранг 2018	Компанія	Країна	2019 Доходи від оборонних продаж (млн \$)	2018 Доходи від оборонних продаж (млн \$)	% змін	2019 Загальні доходи (млн \$)	Частка оборонних доходів
1	1	Lockheed Martin <sup>1</sup>	США	\$56,606.00	\$50,536.00	12%	\$59,812.00	95%
2	2	Boeing	США	\$34,300.00	\$34,050.00	1%	\$76,559.00	45%
3	6	General Dynamics <sup>2</sup>	США	\$29,512.00	\$27,507.00	7%	\$39,350.00	75%
4	3	Northrop Grumman	США	\$28,600.00	\$25,300.00	13%	\$33,841.00	85%
5	4	Raytheon Company <sup>1 3</sup>	США	\$27,448.00	\$25,163.94	9%	\$29,200.00	94%
6	5	Aviation Industry Corporation of China	Китай	\$25,075.38	\$24,902.01	1%	\$66,858.02	38%
7	7	BAE Systems <sup>1</sup>	Велика Британія	\$21,033.27	\$22,477.48	-6%	\$23,370.30	90%
8	8	China North Industries Group Corporation Limited	Китай	\$14,771.60	\$14,777.77	0%	\$68,074.15	22%
9	NEW	L3Harris Technologies <sup>4</sup>	США	\$13,916.98	\$12,303.08	13%	\$18,074.00	77%

<sup>1</sup> Список 100 найкращих компаній сформовано на основі інформації, яку отримує Defence News від компаній, щорічних звітів компаній, аналітиків та досліджень оборонних новин і Міжнародного інституту стратегічних досліджень. Крім того, було проведено опитування компаній, які повідомили про їх загальний річний дохід та доходи від оборонних обладунків, розвідки, внутрішньої безпеки та інших контрактів національної безпеки.

Ранг 2019	Ранг 2018	Компанія	Країна	2019 Доходи від оборонних продаж (млн \$)	2018 Доходи від оборонних продаж (млн \$)	% змін	2019 Загальні доходи (млн \$)	Частка оборонних доходів
10	17	United Technologies Corp. <sup>1 3</sup>	США	\$13,090.00	\$9,310.00	41%	\$77,000.00	17%
11	10	China Aerospace Science and Industry Corporation	Китай	\$12,035.25	\$12,130.93	-1%	\$37,610.17	32%
12	9	Airbus <sup>5</sup>	Нідерланди/Франція	\$11,266.57	\$13,063.82	-14%	\$78,916.36	14%
13	13	Leonardo	Італія	\$11,109.27	\$9,828.51	13%	\$15,429.55	72%
14	14	China Shipbuilding Industry Corporation <sup>6</sup>	Китай	\$11,019.56	\$9,795.47	12%	\$55,097.78	20%
15	12	China Electronics Technology Group	Китай	\$10,148.87	\$10,275.58	-1%	\$32,951.25	31%
16	16	Thales	Франція	\$9,251.68	\$9,575.57	-3%	\$20,596.61	45%
17	15	Almaz-Antey	Росія	\$9,191.60	\$9,660.14	-5%	\$9,651.71	95%
18	11	China South Industries Group Corporation	Китай	\$8,845.87	\$11,963.37	-26%	\$28,550.02	31%
19	20	Huntington Ingalls Industries	США	\$8,119.00	\$7,767.00	5%	\$8,899.00	91%
20	19	China Aerospace Science and Technology Corporation	Китай	\$7,745.57	\$8,138.47	-5%	\$36,223.21	21%
21	NEW	Mitsubishi Heavy	Японія	\$6,570.00	N/A	N/A	\$37,670.00	17%

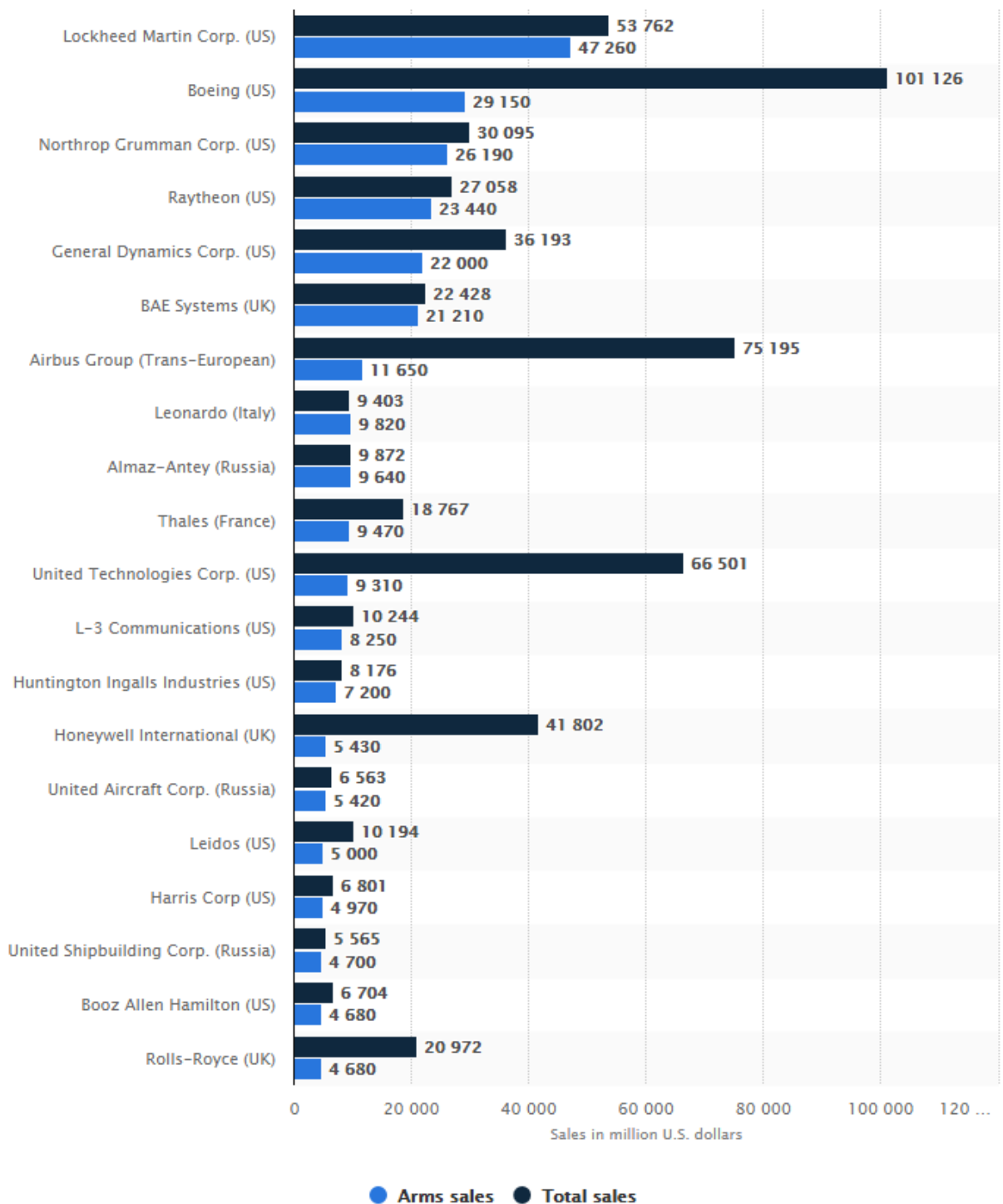
Ранг 2019	Ранг 2018	Компанія	Країна	2019 Доходи від оборонних продаж (млн \$)	2018 Доходи від оборонних продаж (млн \$)	% змін	2019 Загальні доходи (млн \$)	Частка оборонних доходів
		Industries <sup>7</sup>						
22	38	Dassault <sup>8</sup>	Франція	\$5,708.84	\$2,934.43	95%	\$8,171.48	70%
23	21	Leidos	США	\$5,364.00	\$5,378.00	0%	\$11,094.00	48%
24	22	China State Shipbuilding Corporation <sup>6</sup>	Китай	\$5,356.75	\$4,954.07	8%	\$33,495.61	16%
25	25	Honeywell	США	\$5,326.00	\$4,665.00	14%	\$36,709.00	15%

Джерело: Defence News

За оцінками німецької компанії STATISTA, список перших 20 фірм світу – виробників озброєння та військової техніки – виглядає дещо по іншому, але перша п'ятірка така ж (рис. 4).

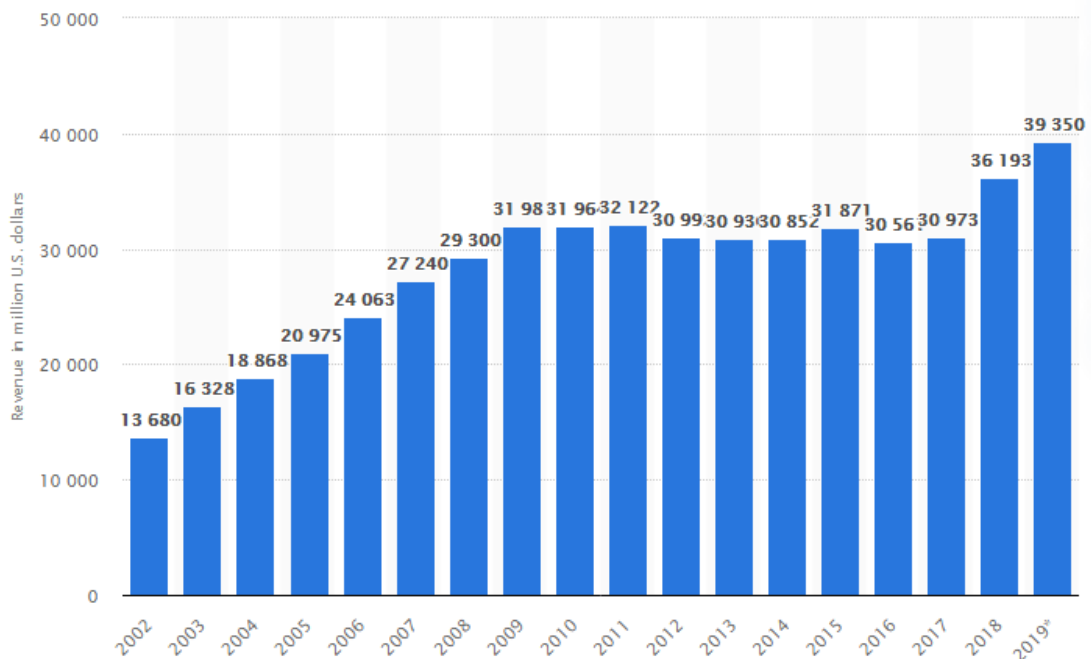
Усі ці фірми в останні роки витрачали суттєві і зростаючі кошти на наукові дослідження і розроблення технологій. Внаслідок цього доходи від військових технологій у 2018 та 2019 рр. теж зросли (рис. 5).

При цьому, динаміка доходів від військових технологій ідентична динаміці витрат на військову сферу (рис. 1 та рис. 5). Слід зауважити, що доходи від військових технологій зростають швидше, ніж витрати на військову сферу у світі. Так, у 2019 р. порівняно з 2018 р. військові витрати зросли на 3,6%, а доходи від технологій – на 8,7%, що говорить про прибутковість військових наукових досліджень.



Джерело: The 20 largest arms-producing and military services companies in the world in 2018, by arms sales. - <https://www.statista.com/statistics/267160/sales-of-the-worlds-largest-arms-producing-and-military-services-companies/>

**Рис. 4** Топ-20 світових компаній, що виробляють військову продукцію та надають військові послуги, у 2018 р. за обсягами продажу за версією STATISTA, млн дол. США



Джерело: Revenue of the defense technology supplier General Dynamics from 2002 to 2019. - <https://www.statista.com/statistics/268819/revenue-of-the-defense-technology-supplier-general-dynamics/>

**Рис. 5 Динаміка доходу від постачання військових технологій за 2002-2019 рр., млн дол. США**

Ще одна прикмета останніх двох років – суперництво між США та Китаєм, яке стало парадигмою міжнародних відносин. Воно формує як стратегічні дебати, так і реальну політичну, військову та економічну динаміку:

- виміри китайсько-американської конкуренції за владу та статус включають зростання загроз із більшою політичною / ідеологічною складовою;

- торговельний конфлікт між США та Китаєм є політичним і тісно пов'язаний із світовим порядком;

- суть технологічного виміру полягає не в тому, хто встановлює стандарти, а в геополітичному прогнозуванні "технополітичних сфер впливу". Розвиток та використання технологій стають частиною системної конкуренції;

- за допомогою відповідних стилів керівництва президенти Трамп та Сі розпалюють двосторонні конфлікти і, кожен по-своєму, завдає шкоди міжнародним правилам та установам;

- китайсько-американське суперництво також підриває міжнародні інститути, такі як Всесвітня організація торгівлі. Поки Вашингтон вийшов з

ряду багатосторонніх угод та міжнародних установ, Пекін розширює свій вплив, зокрема в Організації Об'єднаних Націй.

*Ключові тенденції та драйвери наступного десятиліття [2]:*

- зміна міжнародного порядку, що відзначається посиленням конкуренції та зміщенням світового економічного центру тяжіння до Азії;

- дедалі відчутніші наслідки зміни клімату, що сприяє подальшим змінам в усьому світі. Зміна клімату прискорюється, і зростання глобальної температури поверхні може досягати +1,5°C між 2032 і 2052 роками порівняно з доіндустріальним рівнем [3], а до 2022 року в результаті кліматичних змін та конфліктів більше 200 мільйонів людей можуть потребувати гуманітарної допомоги;

- погіршення стану природного середовища з безпрецедентною втратою біорізноманіття [4];

- вплив технологій: створюються можливості, посилюються потенційні ризики та збільшується свобода діяльності недержавних суб'єктів. Наприклад, капіталізація Apple, Google та Microsoft разом перевищує ВВП Великої Британії [5];

- все більш складний глобальний економічний контекст. Швидке зростання ринків, що розвиваються, означає, що частка G7 у світовому ВВП зменшується. За прогнозами, глобальний «середній клас» зросте з 3,8 млрд осіб у 2018 році до 5,3 млрд до 2030 р. [6];

- збільшення нестабільності та викликів глобальному управлінню. У 2019 р. зафіксовано найбільшу кількість конфліктів у світі з 1946 р. [7], а за останні 10 років більше половини населення світу жило в безпосередньому контакті зі значним політичним насильством або поблизу від нього [8].

## ОГЛЯД ТЕХНОЛОГІЧНИХ ТРЕНДІВ У ВІЙСЬКОВІЙ СФЕРІ

З початку поточного століття глобальне середовище безпеки переживало значні зміни. Все більш багатополярний світ характеризується зростанням сильних держав-акторів, таких як Росія та Китай, а також значною кількістю недержавних збройних формувань і слабких держав по всьому світу. Ці події породили напружені дискусії щодо сучасної та майбутньої глобальної архітектури безпеки.

У цьому контексті увага Стокгольмського інституту проблем миру (SIPRI) та Мюнхенської конференції з питань безпеки приділяється більш глибокому та більш ефективному співробітництву в галузі оборони та безпеки в Європі, на міжнародному рівні, включаючи контроль над ядерними та звичайними озброєннями, боротьбу з тероризмом, транснаціональною організованою злочинністю, співпрацю у сфері розвідки, планування і закупівлі, і стратегічне передбачення.

Основні питання, яких у 2020 році торкалися під час конференцій та симпозіумів з питань миру та безпеки, стосувалися таких технологічних напрямів:

*Кібербезпека і технології.* У світлі нових викликів у XXI столітті Мюнхенська конференція з питань безпеки має на меті забезпечити конструктивний діалог з нагальних питань у кібертехнологічній сфері. У циклі з питань кібербезпеки та технологій обговорюється вплив технологічних змін та шанси і ризику у цифровому світі.

Кібербезпека стала найважливішим пунктом порядку денного міжнародної безпеки в останні роки. Зростаюча увага, яку отримує ця тема, відображається в дискусіях про норми в кіберсфері, занепокоєння щодо великих даних та конфіденційності, щодо безпеки критичної інфраструктури. Одночасно такі технологічні розробки, як штучний інтелект та нові типи озброєнь, мають незліченні наслідки для безпеки – у звичайній війні, кіберпросторі, а також у космічному просторі. Ключовою метою серії “Кібербезпека та технології” є поєднання технологій, політики у секторі безпеки шляхом об’єднання зусиль осіб, що приймають рішення на найвищих рівнях уряду, з наукових, військових кіл, представників приватного сектору та громадянського суспільства.

Покращення кібербезпеки та можливостей кіберзахисту останнім часом стало головним пріоритетом у програмах національної безпеки багатьох європейських держав. Широкий спектр держав створює спеціалізовані агентства з кіберзахисту, збільшуючи людські та фінансові ресурси, пов’язані

з кіберпромисловістю, та розробляє національні стратегії, які іноді включають розвиток наступальних кібер-можливостей.

SIPRI здійснює моніторинг питань, пов'язаних із сек'юритизацією та милітаризацією кіберпростору, а також політикою кіберзахисту та кібербезпеки ряду держав та багатонаціональних органів, включаючи США, Велику Британію, Францію, Росію, ЄС, НАТО, Організацію з питань безпеки та співробітництва в Європі (ОБСЄ) та ООН.

*Технології штучного інтелекту.* ШІ визначено як найбільший технологічний виклик, з яким стикаються країни світу [9], дехто називає його найважливішою технологією, коли-небудь винайденою [10]. Протягом наступних 20 років, як очікується, ШІ буде відігравати значний вплив і значну руйнівну силу завдяки своїм наслідкам.

Китай прагне стати лідером у ключових військових технологіях, таких як ШІ, автономні системи, передові обчислювальні технології, квантові інформаційні науки. Впровадження в Китаї ШІ та квантової комунікаційної мережі демонструє швидкість та масштаби, з якими він має намір застосовувати певні новітні технології.

*Автономні системи зброї.* З 2013 року управління летальними автономними системами зброї (LAWS) обговорювалося в рамках Конвенції ООН про певну звичайну зброю 1980 року. Однак дискусія залишається на ранній стадії, оскільки більшість держав все ще перебувають у процесі розуміння конкретних аспектів та наслідків збільшення автономії в системах озброєнь.

SIPRI вважає, що для розробки концепцій та контролю за автономними системами зброї необхідним є краще розуміння (1) технологічних основ автономії, (2) сучасних програм та можливостей автономії в існуючих системах зброї, (3) технологічних, соціально-економічних, оперативних та політичних факторів, які в даний час дозволяють або обмежують її досягнення.

*Ядерна зброя.* SIPRI відстежує тенденції та розвиток ядерних сил та доктрин, з особливим акцентом на моніторингу глобальних запасів ядерної зброї. Ця робота включає підготовку оцінок кількості та типів боєголовок та супутніх транспортних засобів, що знаходяться у кожній з дев'яти відомих або підозрюваних держав, що володіють ядерною зброєю, та тих, що можуть її мати. Крім того, здійснюється моніторинг національних можливостей ядерної зброї, якщо держави вносять кількісні та якісні зміни до своїх ядерних арсеналів.



Дані про ядерну зброю SIPRI базуються виключно на загальнодоступних матеріалах з відкритим кодом. Сюди входять офіційні джерела (урядові "Білі книги", публікації парламенту та конгресу та офіційні заяви), а також вторинні джерела (звіти та періодичні видання в ЗМІ, торгові журнали). У деяких випадках оцінки запасів ядерної зброї базуються на відомостях про технічні можливості конкретних об'єктів, з яких можна екстраполювати виробничі можливості.

Ключовий висновок: незважаючи на загальне зменшення кількості ядерних боєголовок у 2019 році, усі держави, що володіють ядерною зброєю, продовжують модернізувати свої ядерні арсенали.

*Біологічна зброя.* Увага зосереджується на запобіганні актам тероризму масового впливу та спостереженні та реагуванні на хвороби в Азії. Також розглядаються юридичні, технічні та історичні аспекти впровадження міжнародних заборон проти біологічної війни, включаючи перевірку її невиробництва у національних оборонних науково-дослідних установах, а також наслідки для безпеки технологій подвійного використання та технологій у науках про життя.

*Космічні технології.* Космос є унікальним середовищем. Від космосу на сьогодні залежать можливості військових сил оперативно та ефективно виконувати свої місії.

Різноманітність космічних технологій матиме прямий вплив на майбутні війни. Одним з найбільш важливих трендів є збільшення залежності від технологій ШІ для оброблення і використання великого масиву інформації, отриманої у та з космосу. Ці технології включають використання інших технологій – цифрової реальності (віртуальної, змішаної тощо), підтримки космічних операцій та навчання; оптичного зв'язку між землею та космосом з високою швидкістю передачі даних; вдосконаленої кібербезпеки для запобігання несанкціонованому використанню або переназначенню супутників і роїв; здійснення аналізу, підвищення стійкості (наприклад, щодо сміття, космічної погоди) та поінформованості про ситуацію в космосі.

Відносно новою концепцією є *кібервійна*, хоча Інтернет починався як військова технологія. Кіберпростір став п'ятою ареною війни, окрім суші, моря, повітря та космосу. Дрібномасштабні кібервійни вже відбуваються щодня. Наприклад, американський та британський уряди на початку 2018 року опублікували заяви, в яких звинуватили російський уряд у кібератаці "NotPetya", яка, за їхніми словами, мала на меті дестабілізувати Україну. Більшість кібератак використовують людські помилки із використанням

таких інструментів, як фішинг-електронні листи (згідно з доповіддю, опублікованою в 2018 році фірмою безпеки Proofpoint).

Країни найбільш вразливі до атак, спрямованих на стратегічні активи та інфраструктуру, які порушують інтернет-трафік як засіб для розбурхання ситуації. Загрози кібератак посилюються через відсутність міжнародних угод, які регулюють кібервійну та встановлюють правила цифрових боїв. Як результат, цілі кібератак не обмежуються агенціями урядів-партнерів, а включають приватні організації, такі як електромережі, які часто не мають належного обладнання із кіберзахисту. У лютому 2018 року Генеральний секретар ООН Антоніу Гутерріш закликав встановити глобальні правила, що регулюють кібервійну, з метою мінімізації потенційного впливу на цивільне населення. Він зазначив, що незрозуміло, як, наприклад, Женевські конвенції, на які вже давно зверталися з метою регулювання збройних конфліктів, можуть застосовуватися до кібервійни [11].

З'являється нова область для військових цифрових технологій – *Інтернет речей (IoT)*. НАТО шляхом експериментів, демонстрацій та семінарів продемонстрував, що IoT має відігравати важливу роль у майбутніх військових операціях, включаючи гуманітарну допомогу та ліквідацію наслідків катастроф, боротьбу з тероризмом, розумний фізіологічний моніторинг солдатів і логістику та управління ланцюгами поставок. Наприклад, у випадку стихійного лиха в майбутньому розумному міському середовищі можливість використання безлічі датчиків та інтелектуальних служб у місті може дозволити військовим збирати інформацію набагато швидше, ніж покладатися виключно на розгорнуте зондування та збір інформації. Можливість скористатися таким інформаційним середовищем та використовувати його може бути безцінною для майбутніх військових операцій. Наступною проблемою, яка закономірно виникає, є дослідження різних підходів до інтеграції цих величезних і різнорідних систем і можливостей IoT в існуючі системи військового управління. Без систематичних підходів до інтеграції цих можливостей було б дуже важко використати можливості IoT для підтримки військових операцій [12].

Протягом наступних 20 років можна очікувати появи *чотирьох ключових характеристик передових військових технологій*:

- інтелектуальність: використання інтегрованого ШІ, аналітичних можливостей, орієнтованих на знання, та симбіотичного інтелекту для розроблення руйнівних програм в усьому технологічному спектрі;
- взаємопов'язаність: використання мережі віртуальних та фізичних доменів, включаючи мережі датчиків, організацій, приватних осіб та

автономних агентів, пов'язаних за допомогою нових методів шифрування та розподілених технологій реєстру;

- розподіленість: використання децентралізованого та повсюдного широкомасштабного зондування, зберігання та обчислення для досягнення нових руйнівних військових ефектів;

- цифровізація: цифрове поєднання людського, фізичного та інформаційного доменів для підтримки нових руйнівних ефектів.

## ШТУЧНИЙ ІНТЕЛЕКТ

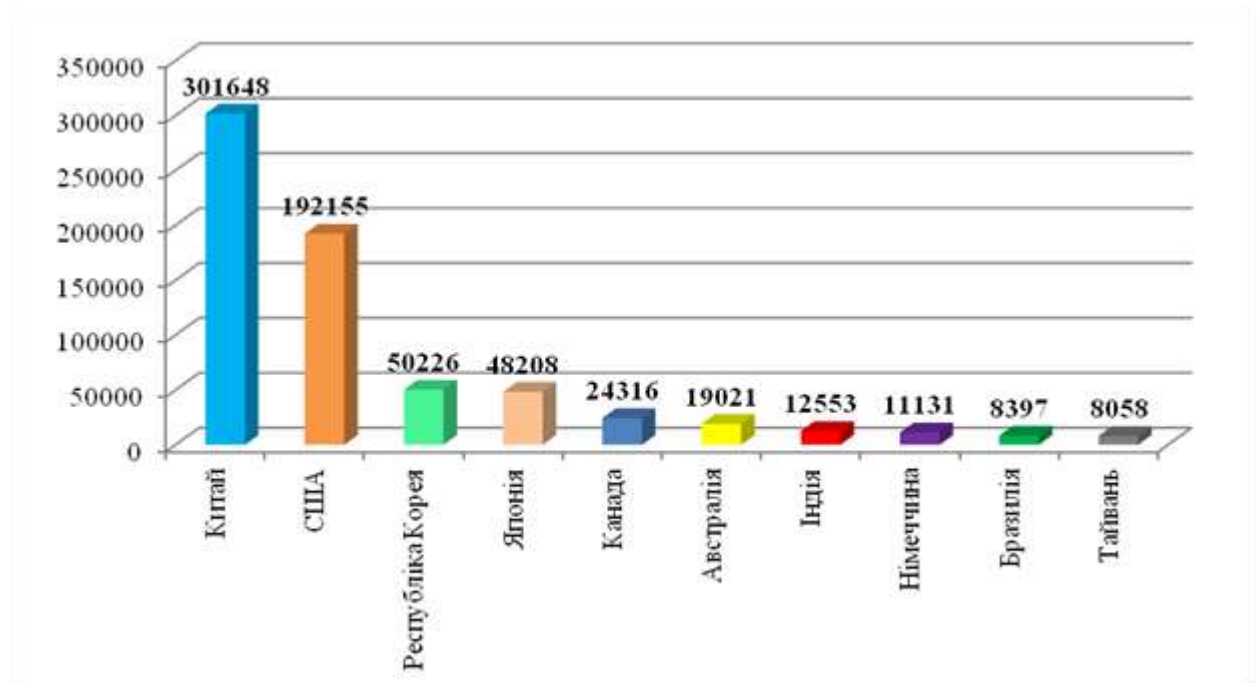
ШІ – це здатність машини відображати подібні людським можливості, такі як міркування, навчання, планування та творчість.

ШІ дозволяє технічним системам сприймати навколишнє середовище, мати справу із зібраною інформацією, вирішувати проблеми та діяти для досягнення конкретної мети. Комп'ютер отримує дані – вже підготовлені або зібрані за допомогою власних датчиків, таких як камера, – обробляє їх і реагує на них.

Системи ШІ здатні адаптувати свою поведінку до певної міри, аналізуючи наслідки попередніх дій та працюючи автономно.

Деякі технології ШІ існують вже більше 50 років, але досягнення в обчислювальній потужності, наявність величезної кількості даних та нові алгоритми призвели до значних проривів ШІ за останні роки.

Серед країн світу найвищим потенціалом у сфері штучного інтелекту володіє Китай – його компанії володіють 17-ю з топ-20-ти правами інтелектуальної власності щодо ШІ та 10-ю з топ-20 наукових публікацій, що відносяться до сфери ШІ [13]. Це ж стосується і військового застосування ШІ (рис. 6).



Джерело: Derwent innovation

**Рис. 6 Топ-10 країн світу за кількістю патентів у сфері військового застосування штучного інтелекту, од.**

У липні 2017 р. Державна Рада КНР розробила детальну стратегію із перетворення Китаю до 2030 р. у «лідера та глобальний центр інновацій в

області штучного інтелекту». Стратегія включає в себе інвестування у дослідження та розробки, які «будуть зміцнювати за допомогою ШІ національну оборону, забезпечувати та захищати національну безпеку». У цій стратегії особлива увага приділена застосуванню ШІ в областях автоматизації бойових дій та прогнозування. У стратегії Пекіна вказувалося, що країна повинна стати світовим лідером в області ШІ до 2030 року.

На виконання завдань цієї стратегії 85% китайських компаній є активними гравцями в сфері ШІ, тобто, компанії, які досягли суттєвого прогресу у впровадженні ШІ в існуючі процеси, або ініціюють пілотні програми. У цілому китайські компанії є лідерами на світовому ринку ШІ (рис. 7).



Джерело: Mind the (AI) Gap. Leadership Makes the Difference. - [https://image-src.bcg.com/Images/Mind\\_the%28AI%29Gap-Focus\\_tcm108-208965.pdf](https://image-src.bcg.com/Images/Mind_the%28AI%29Gap-Focus_tcm108-208965.pdf)

**Рис.7 Частка активних щодо застосування ШІ компаній у передових країнах світу, %**

Воєнно-технічна політика та концентрація Пекіна на ШІ не залишилася поза увагою сусідів по регіону. Індія та Японія планують об'єднати зусилля у розробці військових наземних безпілотних машин та військових роботів як протидію Китаю. Представник індійського Центру штучного інтелекту та робототехніки (CAIR) заявив, що мета спільної роботи – оснащення військових сил відмовостійкими роботизованими системами.

Як і Китай, Росія активно розробляє методи і програми військового застосування ШІ. У даний час розвиток російського ШІ значно відстає від

розвитку Сполучених Штатів Америки та Китаю, оскільки жоден російський відповідний стартап не увійшов до рейтингу 100 [14]. Однак Російська Федерація ініціює плани щодо подолання розриву. У рамках цих зусиль вона оприлюднила національну стратегію щодо штучного інтелекту, яка окреслює 5- та 10-річні орієнтири для вдосконалення знань про ШІ в країні, освітніх програм, наборів даних, інфраструктури та правової системи регулювання [15]. Росія також продовжить свою програму з модернізації оборони з метою роботизувати 30% своєї військової техніки до 2025 року.

Росія створює ряд організацій для розвитку військового ШІ. У березні 2018 року російський уряд оприлюднив порядок денний щодо штучного інтелекту з 10 пунктів, який вимагає створення консорціуму зі штучного інтелекту та великих даних, фонду аналітичних алгоритмів та програм, державної навчальної та освітньої програми зі ШІ, спеціальної лабораторії штучного інтелекту, а також Національного центру штучного інтелекту [16]. Крім того, Росія створила Фонд перспективних досліджень<sup>2</sup>, подібний DARPA, та ініціювала щорічну конференцію на тему "Роботизація збройних сил Російської Федерації"[17].

Російські військові досліджували ряд застосувань штучного інтелекту з акцентом на напівавтомні та автономні машини, побудували бойовий модуль для наземної техніки, який здатний самостійно визначати цілі і, можливо, цільовий рівень взаємодії, і планують розробити набір автономних систем на основі ШІ.

Також Росія передбачає впровадити ШІ у повітряні, морські та підводні апарати, створювати рої. Вивчається можливість використання ШІ для дистанційного зондування і радіоелектронної боротьби, для внутрішньої пропаганди та для інформаційних операцій проти супротивників [18].

На початку лютого 2018 року військове відомство США опублікувало «Короткий зміст Стратегії Міністерства оборони зі штучного інтелекту на 2018 рік». У стратегії згадується застосування ШІ для підвищення загальної ситуаційної обізнаності та розпізнавання, що виникають і є неочевидними щодо небезпек для операторів в усіх сферах їх діяльності. Йдеться про контроль за складними об'єктами інфраструктури та озброєння, військової і спеціальної техніки (ОВСТ) з метою моніторингу і прогнозування їх стану для запобігання, тим самим, техногенних катастроф, аварій та недопущення втрати функціональних можливостей ОВСТ. Тобто в Стратегії озвучена роль

---

<sup>2</sup> Фонд перспективних досліджень створено на виконання Федерального закону від 16.10.2012 № 174-ФЗ «Про Фонд перспективних досліджень». Його метою є сприяння науковим дослідженням і розробкам в інтересах оборони і безпеки держави шляхом досягнення якісно нових результатів у військово-технічній, технологічній і соціально-економічній сферах, створення інноваційних технологій і виробництва високотехнологічної продукції військового, спеціального і подвійного призначення.

ШІ тільки у мирний час. Однак і для військового часу фахівцями США визначені завдання для ШІ.

Бюджетний запит Міністерства оборони щодо інформаційних технологій і кіберпростору на 2021 р. становить 49,5 млрд доларів, у т.ч. на діяльність у кіберпросторі – 9,8 млрд дол., що на 0,2 млрд дол. (2,1%) більше, ніж у 2020 р. Передбачається забезпечити інфраструктурою, ресурсами та інструментами кібервоїнів для захисту, безпеки інформаційних мереж і систем, а також для можливості проводити наступальні операції.

*Види ШІ:*

- Програмне забезпечення: віртуальні помічники, програмне забезпечення для аналізу зображень, пошукові системи, системи розпізнавання мови та обличчя.

- "Втілений" ШІ: роботи, автономні машини, безпілотники, Інтернет речей.

ШІ у повсякденному житті:

- Інтернет-магазини та реклама.
- Персоналізовані рекомендації людям на основі, наприклад, їх попередніх пошуків та покупок або іншої поведінки в Інтернеті;

- У торгівлі: оптимізація продукції, планування запасів, логістика тощо.

- Веб-пошук – пошукові системи, що самовдосконалюються на величезному обсягу даних.

- Цифрові особисті асистенти: смартфони, що використовують ШІ для надання послуг, є максимально актуальними та персоналізованими; віртуальні помічники, які відповідають на питання, надають рекомендації та допомагають організувати щоденну рутинну працю.

- Машинні переклади – програмне забезпечення для мовного перекладу, засноване на письмовому або розмовному тексті, покладається на штучний інтелект для забезпечення та вдосконалення перекладів. Це також стосується таких функцій, як автоматичне субтитрування;

- Розумні будинки, міста та інфраструктура – розумні термостати економлять енергію, тоді як розробники розумних міст сподіваються регулювати рух для покращення зв'язку і зменшення пробок.

- Автомобілі – самокеровані транспортні засоби, функції безпеки в автомобілях на основі штучного інтелекту, автоматизовані датчики, що виявляють можливі небезпечні ситуації та аварії.

- Навігація, яка в основному забезпечується штучним інтелектом.

- Кібербезпека. Системи ШІ можуть допомагати розпізнавати та боротися з кібератаками та іншими кіберзагрозами на основі постійного

введення даних, розпізнавання закономірностей та зворотного відстеження атак і т. д.

З моменту свого заснування в середині 1950-х років ШІ пройшов *три цикли розвитку технологій*:

- початковий – підхід, заснований на правилах (дерева рішень, булева і нечітка логіка), наприклад, експертні системи [19];
- другий – розробка та застосування статистичних методів (тобто навчання під наглядом, без нагляду та підкріплення). Методи машинного навчання були дуже успішним і лежать в основі всього – від фільтрації спаму електронною поштою до веб-пошуку в Інтернеті;
- третій – використання біоінспірованих методів навчання (нейронні мережі, глибинне навчання), значний успіх у сферах зондування та сприйняття [20].

У той час, як продовжуються успіхи в методах глибинного навчання, розробляються нові напрями досліджень, включаючи нейроморфні обчислення, які намагаються більш точно імітувати нервову структуру та роботу людського мозку [20], а також протиборчу машину, навчання, яке прагне зрозуміти, як намагатися заплутати системи ШІ [21]. Інший перспективний напрям – це імовірнісні обчислення, призначені для боротьби з невизначеністю, двозначністю та протиріччями у природному світі.

Дослідження в цих областях включають нові методи машинного та глибинного навчання, орієнтовані на використання невеликих навчальних наборів та пояснюваність. Ще одним важливим напрямом досліджень і розробок стане розробка нових алгоритмів машинного та глибинного навчання, заснованих на квантовій інформатиці та квантових комп'ютерах. Продовження досліджень та розробок нових та більш універсальних алгоритмів буде критично важливим для підтримання поточного імпульсу досліджень ШІ та виведення ШІ за його поточні практичні обмеження.

Існують можливості досліджень та розробок для значного розширення аналізу великих наборів даних, включаючи ті, що пов'язані з обробкою, синтезом та аналізом даних датчиків. Очікуваний швидкий вибух оцифрованих даних зробить використання ШІ (та його похідних) ще більш корисним та практично необхідним.

Програма «Партнер з досліджень в області штучного інтелекту» (AIRA) є частиною широкої ініціативи DARPA із розробки і застосування технологій штучного інтелекту «третьої хвилі», стійких до розрізнених даних



і хакерських атак (IP-спуфінгу), які включають знання предметної області шляхом генеративних контекстних і пояснювальних моделей [22].

У 2020 році очікується вироблення 44 трильйонів гігабайт цифрових даних, при цьому щорічний темп приросту повинен становити близько 60%, а практично – понад 500. Без ШІ фізичні особи та організації вимушені будуть припинити намагання перетворити ці великі обсяги даних у дієві знання.

Якість даних, зокрема, є найважливішим питанням ШІ. Довіра до великих наборів даних є важливим елементом багатьох алгоритмів ШІ та значним внеском у природу багатьох програм ШІ. Проводяться дослідження щодо розробки більш пристосованих та ефективних алгоритмів машинного навчання, які потребуватимуть менш маркованих даних і здатні робити висновки щодо розріджених або суперечливих даних, одночасно роблячи їх більш легкими для навчання, більш стійкими до непередбачуваних реальних умов та універсальними для нових середовищ [23].

Подібним чином проводяться дослідження із оцінювання системи ШІ у разі отримання несправжніх даних, що може бути використано для маніпулювання супротивником [24]. Оскільки системи ШІ стають повсюдними та лежать в основі прийняття рішень у складних системах, необхідність у розробці відповідних контрзаходів та алгоритмічної стійкості буде вкрай необхідною.

Розробка симбіотичного ШІ (тобто людиноцентричного), завдяки якому люди та когнітивні машини працюють разом як надійні партнери в складній гібридній системі, є важливим завданням для дослідження [24]. Фундаментальні дослідження та розробки необхідні для покращення розуміння людської мови, вилучення семантичної інформації, властивої широкому спектру засобів масової інформації, та реагування на невербальні аспекти спілкування. Такі можливості також дозволять більш природну взаємодію та партнерство, але також вимагатимуть інтеграції аналогів до людського сприйняття у фізичній (наприклад, зір) та людській сферах (наприклад, емоції), разом із розвитком машинного здорового глузду (тобто впровадження апріорних знань [24]). Це також потребуватиме розробки систем, здатних задавати питання, розмірковувати, пропонувати декілька варіантів, покращувати навчання та чітко пояснювати рішення чи процес обговорення.

*Драйвери росту.* Протягом 20 років, як очікується, ШІ буде мати все більш значний вплив завдяки *таким факторам:*

- посилена цифровізація та наявність у результаті (дуже) великих наборів даних, включаючи загальнодоступні дані для системного навчання та розробок;
- широке поширення та використання в кіберфізичних системах;
- нові сфери застосування, зумовлені більшими інвестиціями та ширшим впровадженням методів ШІ;
- прийняття рішень та оптимальний контроль (наприклад, енергосистеми, інвестиції тощо);
- обчислення / обчислювальні технології, всюдисущі датчики, дизайн бази даних,
- інструменти для розвитку, хмарні обчислення, нові алгоритмічні підходи та використання ШІ для завантаження
- розвиток ШІ;
- розробка вдосконалених засобів аналізу великих даних та комп'ютерного зору.

*Драйвери розвитку військового ШІ.* У військовій сфері ШІ значно вплине на можливості та сили армій переважно завдяки використанню вбудованого ШІ в інших супутніх технологіях, таких як віртуальна / доповнена реальність; квантові обчислення; автономність, моделювання, простір; дослідження матеріалів; виробництво та логістика; аналіз великих даних. ШІ матиме перетворюючий вплив на ядерну, аерокосмічну, кібермережу, матеріали та біо-технології. Ці наслідки матимуть такий же стратегічний вплив, що і впровадження ядерної зброї. Крім того, надмірна залежність від систем штучного інтелекту також призведе до нових загроз і уразливих місць та започаткує гонку озброєнь в галузі штучного інтелекту.

Деякі потенційні зони впливу протягом наступних 20-ти років очікуються в таких областях:

- C4ISR: Військові підрозділи використовуватимуть надійні автономні системи з підтримкою ШІ як віртуальних помічників, здатних виконувати завдання, які вважаються небезпечними або дорогими.
- Зброя та ефекти: Вважається, що ШІ може бути потенційно корисним для планування траєкторій, уникнення зіткнень, вибору зброї, оцінки шкоди від бою та координації ефектів.
- Планування: ШІ підтримуватиме розробку аналітичних рішень для довгострокового планування, включаючи підтримку прийняття складних рішень тощо.

В інтересах робототехніки ШІ буде все більше розвиватися. Експерти і вчені не сумніваються, що повністю автономні бойові системи, які самі будуть шукати ціль і приймати рішення, з'являться у найближчі 20-30 років.

Ступінь їхньої автономності можна розділити на три категорії: «людина у системі управління» (human-in-the-loop), «людина над системою управління» (human-on-the-loop) і «людина поза системою управління» (human-out-of-the-loop).

*Ризики і загрози.* Використання ШІ збільшить потенційний вплив кібер- та інформаційних атак.

Додатковими загрозовими аспектами майбутніх розробок ШІ є:

- Кіберсистеми ШІ особливо вразливі до кібератак, завдяки чому незначні, навмисні зміни можуть призвести до помилкових рекомендацій або неоптимальних дій.

- Інформація: Досягнення технологій обробки мови та синтезу, швидше за все, дозволять виявляти доброзичливу або ворожу інтонацію.

- Всім вибуховим пристроям інтелектуальне навчання дасть можливість бути менш сприйнятливими до традиційних контрзаходів.

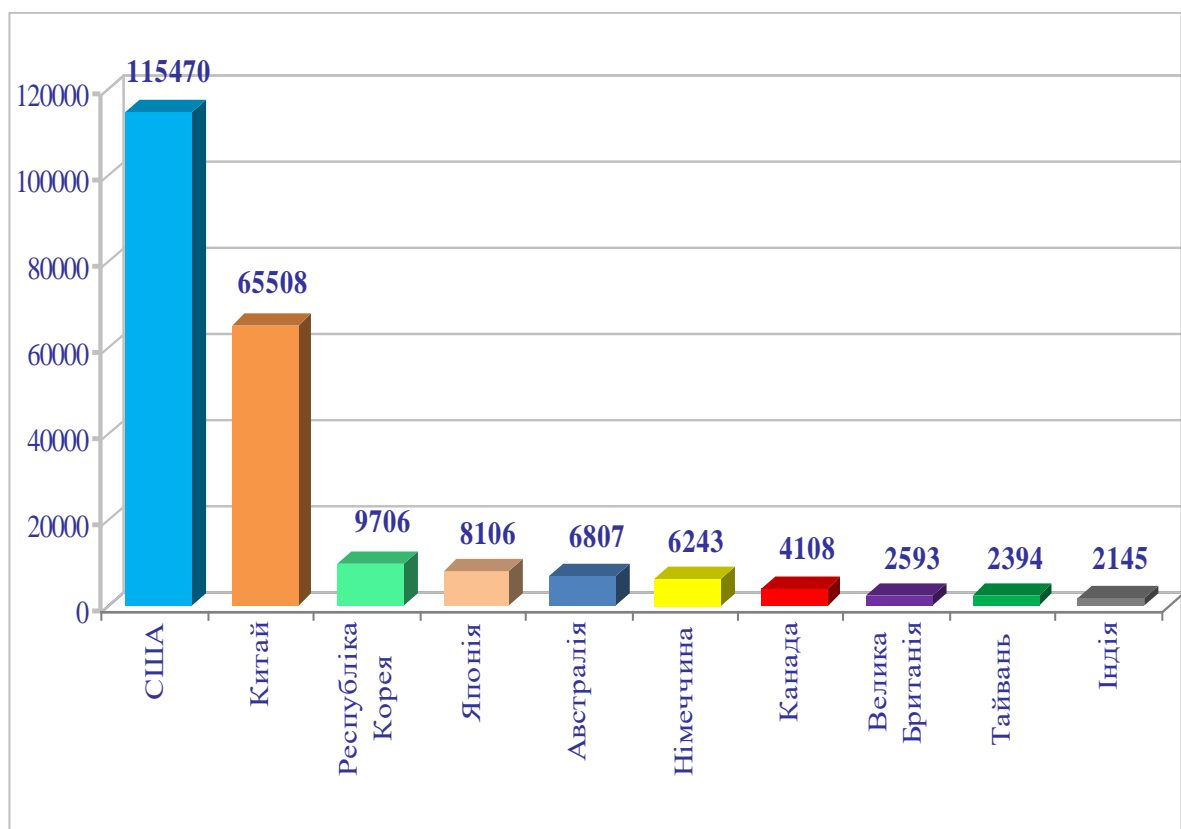
*Прогноз напрямів розвитку технологій* – розширені алгоритми (машинне та глибоке навчання, нейроморфні та імовірнісні обчислення), симбіоз людина-машина (інтерфейс, орієнтований на людину, візуалізація, пояснюваність, командна динаміка), інфопростір (створення зброї за допомогою ШІ, напр., глибокі підробки) та розроблення заходів протидії, напр., підтримка довіри та протидія вразливості) тощо.

*Ринкові перспективи.* До 2027 р. світовий ринок ШІ досягне 400,2 млрд дол. США із середніми темпами росту у 41,5% [24].

## КІБЕРБЕЗПЕКА І ТЕХНОЛОГІЇ КІБЕРПРОСТОРУ

Кіберзагрози, що постійно розвиваються і стають все більш витонченими, а також зростаюча кількість пристроїв, підключених до Інтернету, роблять завдання оцінки кіберризиків безпеки та управління ними все більш актуальними. Ця проблема ще більше посилюється у сфері оборони і національної безпеки, де порушення ІТ-безпеки можуть мати серйозні наслідки.

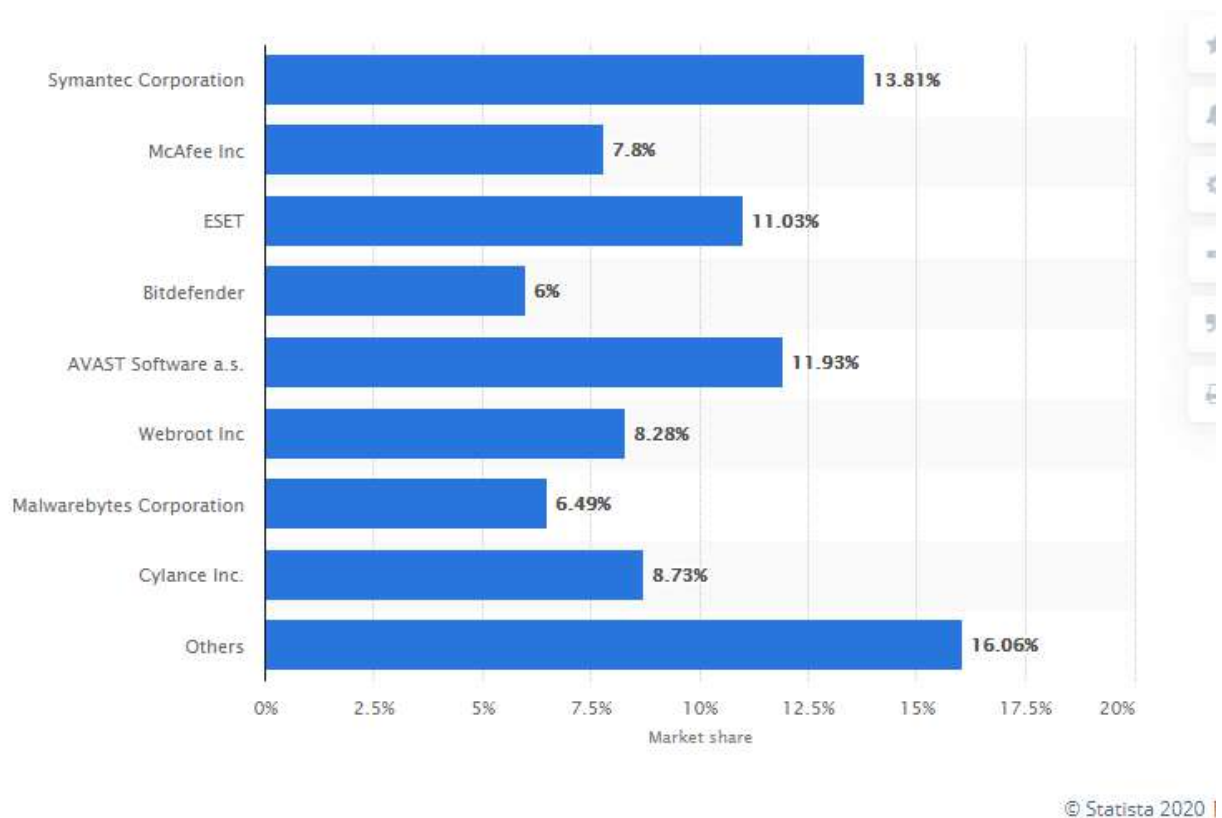
Серед країн світу найвищим потенціалом у сфері кібербезпеки володіють США, Китай, Корея. Серед країн ЄС – Німеччина та Велика Британія (рис. 8).



Джерело: Derwent innovation

**Рис. 8** Топ-10 країн світу за кількістю патентів у сфері програм із військової кібербезпеки, од.

За даними STATISTA, найвища частка ринку, яку займають постачальники протівірусного програмного забезпечення для Windows, станом на квітень 2020 року, належала корпорації Symantec (США) із 13,81 % ринку антивірусного програмного забезпечення. На другому місці компанія AVAST Software із Чехії, на третьому – ESET (Словаччина) (рис. 9).



Джерело: Market share held by the leading Windows anti-malware application vendors worldwide, as of April 2020 [Електронний ресурс]. – Режим доступу: <https://www.statista.com/statistics/271048/market-share-held-by-antivirus-vendors-for-windows-systems/>

**Рис. 9 Частки ринку топ-8 світових компаній із розроблення антивірусних програм, %**

Шкідливе програмне забезпечення може включати знищення або збір даних, небажану рекламу або створення пристрою вразливим до небажаного зовнішнього контролю. Троянські програми та хробаки є найпоширенішими методами зараження шкідливими програмами для компрометації комп'ютерів у всьому світі.

Китай, Тайвань та Туреччина – країни з найвищим рівнем заражених шкідливими програмами комп'ютерів. Швеція, Норвегія та Японія належать до країн з найнижчим рівнем зараження шкідливим програмним забезпеченням [25].

Кіберстратегія Міністерства оборони США (прийнята у 2018 р.) визначає п'ять цілей в області кіберпростору, серед яких дві стосуються кібербезпеки:

- стримування, запобігання або припинення зловмисної кіберактивності, націленої на критичну інфраструктуру США;

- захист інформації і систем Міністерства оборони, в тому числі в мережах, які не належать Міністерству оборони, від кібершпіонажу і зловмисної кіберактивності.

Бюджет діяльності в області кіберпростору на 2021 фінансовий рік [26] (9,8 млрд доларів США) продовжує ґрунтуватися на цілях, викладених у Стратегії цифрової модернізації (DMS), впровадженні інновацій для отримання конкурентних переваг, підвищенні ефективності і можливостей, розвитку кібербезпеки для посилення гнучкості і стійкості, а також на розвитку талантів для цифрової діяльності.

Цей бюджет включає фінансування наукових розробок у сфері кібербезпеки у розмірі 5,4 млрд дол. США та передових досліджень і розробок щодо кіберпростору на суму 0,6 млрд дол. США.

Ці ресурси підтримують програми і заходи, направлені, зокрема, на:

- захисні операції у кіберпросторі;
- захист інформаційної мережі (DoDIN).

4 вересня 2020 р. у США затверджена Директива про космічну політику-5 (Space Policy Directive-5, or SPD-5), що сприятиме розвитку операцій із захисту космічних систем від кіберзагроз [27].

Директива гарантує, що уряд США сприятиме захисту американських космічних систем та можливостей від кіберзлочинців та загроз. Як продовження Стратегії національної безпеки та Національної кіберстратегії, ця Директива визначає такі принципи кібербезпеки для космічних систем:

- Космічні системи та їх підтримуюча інфраструктура, включаючи програмне забезпечення, повинні розроблятися та експлуатуватися з використанням інженерної техніки, яка базується на оцінці ризиків.

- Оператори космічних систем повинні розробити або інтегрувати плани кібербезпеки для космічних систем, що включають можливості захисту від несанкціонованого доступу; зменшити вразливість систем управління, управління та телеметрії; захищати від перешкод та спуфінгу зв'язку; захистити наземні системи від кіберзагроз; сприяти прийняттю відповідних гігієнічних практик кібербезпеки; керувати ризиками ланцюга поставок.

- Вимоги та норми кібербезпеки космічної системи повинні використовувати широко прийняті найкращі практики та норми поведінки.

- Власники та користувачі космічних систем повинні співпрацювати з метою сприяння розробці найкращих практик та підходів до пом'якшення наслідків.

- Оператори космічних систем повинні здійснювати відстеження та врахування ризиків під час реалізації вимог до кібербезпеки.

#### *Напрями сучасних досліджень у сфері кібербезпеки*

*США:* фінансуються дослідження у таких основних сферах: управління кінцевими точками; управління ідентифікацією, обліковими даними та доступом (ICAM); розробка корпоративних безпечних додатків (DEVSECOPS); навчання / підвищення кваліфікації та культури кіберпрацівників; внутрішня безпека; міждоменні рішення для включення мереж партнерів; управління ризиками ланцюга поставок; шифрування; системи військових винищувачів, командування, управління та зв'язок (СЗ); інша критична інфраструктура DoD.

Бюджет кібербезпеки на 2021 фінансовий рік впроваджує важливі ініціативи:

розвиток рішень для шифрування нового покоління і модернізації мереж;

кіберстійкість платформ для виконання завдань шляхом фінансування програм і заходів, спрямованих на просування кібербезпеки, операцій в кіберпросторі, а також передових кібер-досліджень і розробок;

модернізацію та розгортання криптології для наступного покоління систем і платформ;

захист точок обміну інформацією між декількома доменами безпеки для забезпечення конфіденційності, цілісності та доступності міждоменних систем та інформації, що проходить через ці домени;

модернізацію управління ідентифікацією та доступом до облікових даних (ICAM) для узгодження з новими технологіями та архітектурою;

розвиток хмарних обчислень і технологій, які дозволять забезпечити швидкий доступ до інформації, краще прийняття рішень, розширення військових переваг. Оптимізоване корпоративне хмарне середовище також забезпечує платформу для розширених можливостей, таких як ШІ та машинне навчання, які необхідні для збільшення швидкості прийняття рішень та летальності. Використання хмарних технологій змінює спосіб розвитку, розгортання та експлуатації систем та служб Міністерства оборони.

*Велика Британія:* Технології ШІ та управління безпекою і реагуванням (SOAR) – основа інвестиційних стратегій лідерів. Наступні перспективні напрями – швидкість виявлення, швидкість відновлення, швидкість реакції.

ЄС: Бездротова безпека; віддалений доступ / VPN; IoT Security, захист ПК / мобільних пристроїв / кінцевих точок; мобільна безпека / управління пристроям, фільтрування та моніторинг вмісту; брандмауери / брандмауери NextGen; єдине управління загрозами (UTM); антиспам, антивірус / хробак / шкідливе програмне забезпечення; безпека резервного копіювання / зберігання [28].

Майбутня програма "Цифрова Європа" на період 2021-2027 рр. планує інвестувати 1,9 млрд євро у підвищення потенціалу кібербезпеки, покращання її інфраструктури та інструментів в ЄС.

Передбачаються розробки із збільшення взаємозалежності пристроїв та мереж і мережевих зв'язків, автентифікації, криптографії, інноваційних рішень щодо інструментів контролю конфіденційності.

*Драйвери розвитку:*

- швидкий розвиток космічного сектору, специфічна глобальна конкуренція у цьому секторі;
- доступ та використання космосу з високим рівнем автономії;
- зростаюча кількість кібератак і кіберзлочинів.

*Перспективні напрями розвитку технологій:* штучний інтелект (ШІ), компоненти та матеріали, зокрема напівпровідники, космічні системи, великі дані, роботи, космічні робототехнічні технології. А також: 1) прості та безпечні методи автентифікації (зменшення потреби в «надмірній ідентифікації», не обмежуючи при цьому безпеку та анонімність користувача, або, навпаки, пришвидшення майбутнього багатоцільових електронних посвідчень); 2) захист конфіденційності, цілісного рішення із збалансування потреб постачальників онлайн-послуг, постачальників послуг конфіденційності та кінцевих користувачів; 3) пост-квантова криптографія [29], високопродуктивні суперкомп'ютери, 5G [30].

*Перспективи ринку:* глобальний ринок кібербезпеки досягне \$296,5 млрд до 2027 року [31] із темпом росту у 8,9% щорічно протягом 2020-2027 рр.

Сегмент безпеки кінцевих точок зростатиме із темпом у 10,4% щорічно і досягне \$100,2 млрд. Сегмент хмарної безпеки зростатиме на 8,3% щорічно.

Ринок кібербезпеки в США оцінюється в 44 млрд дол. США в 2020 році. Прогнозується, що Китай, друга за величиною економіка у світі, до 2027 року досягне прогнозованого розміру ринку у 70 млрд дол. США із щорічним темпом зростання у 13,6% протягом періоду 2020-2027 рр. Серед



інших вартих уваги ринків – Японія та Канада, кожен з яких зростатиме на 4,8% та 7,9% відповідно протягом 2020-2027 років. У межах Європи Німеччина зростатиме приблизно на 5,8% щорічно.

У глобальному сегменті *хмарної безпеки* США, Канада, Японія, Китай та Європа забезпечать щорічне зростання на 7,7% і досягнуть до 2027 р. обсягу ринку у 40,9 млрд дол. США (24,3 млрд дол. США у 2020 році). Китай залишатиметься одним із найбільш швидкозростаючих у цій групі регіональних ринків. Ринок Азіатсько-Тихоокеанського регіону до 2027 року досягне 41,4 млрд дол. США, тоді як ринок Латинської Америки протягом цього періоду збільшиться на 9,8%.

## АВТОНОМНА ЗБРОЯ ТА РОБОТОТЕХНІКА

Автономія – це здатність системи реагувати на невизначені ситуації шляхом самостійного складання та вибору варіанту дій серед різних напрямів для досягнення цілей, заснованих на знаннях та контекстуальному розумінні світу, самого себе та ситуації. Автономія характеризується ступенями самонаправленої поведінки (рівнями автономії), починаючи від повністю ручного до повністю автономного [32, 33]. Робототехніка – це вивчення проєктування та побудови автономних систем, що охоплюють усі рівні автономії (включаючи повний людський контроль). Безпілотні машини можуть дистанційно керуватися людиною або діяти автономно залежно від місії. Їхнє використання можливе у недоступних районах, для постійного спостереження, із здійснення підтримки солдатів, для більш дешевих, автоматизованих логістичних поставок.

Автономія спирається на різноманітні технології, але, насамперед, на програмне забезпечення і штучний інтелект.

До автономного озброєння відносяться:

*Ударні безпілотники* та інші автономні системи із зниженим рівнем людського контролю, зокрема БПЛА **різних класів** та невеликі рої.

*Системи протиповітряної оборони* – використовують радар для виявлення і відстеження вхідних загроз (ракет або літаків противника), а також керовані комп'ютером системи нападу, які можуть визначати пріоритети, вибирати і потенційно автономно атакувати ці загрози.

*Системи активного захисту* (APSs) – призначені для захисту бронетехніки від протитанкових ракет або снарядів. APS поєднує систему датчиків, як правило, з радіолокаційним, ІЧ або УФ датчиком, що виявляє снаряди, що підлітають до бронетехніки, із системою управління вогнем, яка відстежує, оцінює і класифікує вхідну загрозу.

*Роботизовані гармати*, які можуть автоматично виявляти, відслідковувати та (потенційно) атакувати цілі.

*Керовані боєприпаси*, які також називаються розумними бомбами або прецизійними боєприпасами, – це боєприпаси, які можуть коригувати траєкторії польоту.

*Роботизовані «боєприпаси»* – гібридний тип системи зброї, яка має риси керованих боєприпасів та безпілотних повітряних систем (UCAS), тобто можуть знаходити ціль і потім завдавати удару по ній.

Найвищим потенціалом із розроблення автономної зброї і військової робототехніки володіють США, Російська Федерація, Ізраїль, які мають найбільшу кількість патентів за країною розроблення технологій.

З 2013 року управління летальними автономними системами зброї (LAWS) обговорювалося в рамках Конвенції ООН про певну звичайну зброю 1980 року. Однак дискусія залишається на ранній стадії, оскільки більшість держав все ще перебуває у процесі розуміння конкретних аспектів та наслідків збільшення автономії у системах озброєнь.

У найближчі роки передбачається розроблення наземних робоплатформ легкого, середнього (~10 тонн) і важкого класу (~30 тонн), які зможуть діяти у зв'язці із класичними підрозділами. Десятитонні системи займуть нішу між малими і великими функціональними робоплатформами, які зможуть нести на борту як вантажі, так і озброєння.

Розробники займуться поетапним розширенням "повноважень" робототехніки: рівень розвитку технологій дозволяє системам здійснювати розвідку, наведення і ураження сил супротивника без участі людини. Мова йдеться про інтеграцію даних з різних носіїв, транспортування вантажів, розвідку, координацію наземних робоплатформ і авіації і навіть вогневого ураження сил противника.

Незважаючи на те, що представники ВС США і більшості американських оборонних компаній заявляють про те, що рішення про застосування летальної зброї завжди буде приймати людина, поява повністю автоматизованих комплексів здається неминучим – як мінімум тому, що відповідні розробки веде більшість розвинених країн, включаючи Китай.

У 2019 ВВС у США прийнято програму Vanguard, що включає в себе проекти Skyborg (дрони для пілотованої авіації), розробку експериментальних супутників Navigation Technology Satellite-3 та ініціативу «Золота орда» (Golden Horde), покликану забезпечити можливості ройової взаємодії "розумних" бомб.

«Золота орда» розвивається паралельно з проектом Collaborative Small Diameter Bomb – йдеться як про ройову взаємодію, так і про надання боєприпасам часткової автономності. Як очікується, бомби зможуть самостійно перемикатися на більш пріоритетні цілі, сповістять "колег" про зміни траєкторії польоту, замістять собою збиті противником боєприпаси, і, можливо, навчатися самостійно уникати ряду загроз.

*Драйвери розвитку військових технологій автономності*

Використання БПЛА різних класів та ступеню автономності, збільшення використання невеликих роїв БПЛА принесе значні переваги для наступальних та оборонних операцій.

Автономні системи призведуть до змін у:

1) структурі сили: БПЛА та автономні програмні агенти замінять людей у небезпечних середовищах. Посилене використання автономних систем сприятиме розвитку відповідних військових навичок, організаційних / силових структур та підготовки персоналу;

2) ефективності: застосування системної концепції, що дозволить побудувати мережі наступного покоління та вдосконалений ШІ, який легко інтегрує різні технологічні системи людини в єдину та цілеспрямовану одиницю. Швидке виготовлення (наприклад, 3D / 4D друк на комбінованих матеріалах) забезпечить виготовлення деталей на замовлення системи;

3) контрзаходах: збільшення використання БПЛА та роїв на полі бою потребуватимуть додаткових засобів захисту з можливістю протидії безпілотникам шляхом електронної протидії, кібернетичного, кінетичного ураження, спрямованої енергетичної зброї, використанню роїв перехоплювачів.

Розвитку майбутніх технологій сприятиме використання автономних систем:

у вигляді роїв як витратний актив, наприклад, для проникнення у захищені райони через насичення оборонних споруд або для захисту критично важливих активів;

для транспортування пасажирів та вантажів на полі бою, особливо у відносно невеликих кількостях, які застосовуватимуться у тактичних ситуаціях;

для покращання ситуаційної обізнаності завдяки розосередженим, стійким до засобів ураження, малопомітним транспортним засобам. Очікується збільшення використання у порівняно нових областях ведення бойових дій, таких як космос та кіберсередовище;

для підвищення летальності атаки: велика кількість недорогих систем та вдосконалене об'єднання людей та машин значною мірою поліпшить проєкцію сили. Озброєний БПЛА забезпечить боєздатність у повітряному бою не піддаючи пілота ризику. Зброю може носити сам БПЛА або інтегруватися до літака способом, подібним до повітряної крилатої ракети. БПЛА можуть використовуватися для атаки високоцінних, морських або наземних цілей;

для підвищення маневреності: збільшення тактичної та оперативної спритності завдяки збільшенню присутності автономних систем, кількості (роїв) та зменшення потреб у логістиці;

для зменшення бойових втрат, швидкій медичній допомозі, більшої операційній ефективності і пошуково-рятувальних місій;

для посилення стійкості: поєднання гнучких виробничих та автономних систем може дати можливість автоматизованої логістичної підтримки в небезпечних або ізольованих операційних середовищах;

для регулярних або спеціальних операцій у нетрадиційних та / або асиметричних середовищах загрози, забезпечуючи можливості розвідки (ISR) у складних операціях. Інформація надаватиметься у режимі реального часу, безпосередньо підтримуватиме процеси прийняття командних рішень та зменшувати ризик для військових дій;

для здійснення автономними програмами кібернаступальних та оборонних операцій.

На додаток до БПЛА, розробка нових автономних підземних транспортних засобів буде необхідною для сухопутних військ, особливо тих, що діють у міських умовах. Такі транспортні засоби потребуватимуть навігації мережами тунелів, каналізації, печер та інших міських підземних середовищ.

Для морських операцій застосування автономних систем включає: протидію мінам, ISR у забороненій зоні, протичовнову війну, характеристики навколишнього середовища, оперативний обман. Середовище океанів особливо складні – тиск, температура, навігація та корозія, а також тривале експлуатаційне розгортання. Для цієї ролі особливо добре підходять підводні планери далекої дії.

*Загрози.* Рівні або близькі за розвитком конкуренти використовуватимуть ті самі переваги і технології, що потенційно може скасувати значення автономних сил.

#### *Прогноз напрямів розвитку технологій*

Дослідження та технології охоплюють широке коло задач в області проектування систем, датчиків, інтерфейсів, контрзаходів, людського контролю та додатків, зокрема:

##### 1. Системи:

малопомітні транспортні засоби та системи наступного покоління; нові двигуни; космічні та гіперзвукові системи; малопотужні, менш дорогі та високочутливі датчики; оптимізована мережа розподілу;

збір ISR; приманки; підвищена мініатюризація; нові кібер-фізичні імунні системи; соціальні боти; застосування в складних динамічних середовищах у фізичній (повітря, море, земля, космос), людській (соціальній) та інформаційній (кібер) областях.

Сфера особливої уваги: автономні гіперзвукові апарати; біо-, мікро- та міні-повітряні апарати; невеликі супутники (smallsats); гібридно-електричні авіаційні силові установки; технологія гіперспектральної візуалізації з високою роздільною здатністю для спостереження; мініатюризація радіочастотного сенсора; плазмоніка для зменшення розміру IR детектора; швидке моделювання 3D-середовища; використання роботизованих приманок;

2. Об'єднана система людина-машина: підвищення продуктивності праці людини, співпраця людина-машина, оптимізована соціально-технічна інтеграція, нові інтерфейси та прилади управління, у т.ч. мікроелектроніка.

3. Контрзаходи: радіочастотна зброя високої потужності, зброя направленої енергії (DEW); протидія роям; приманки; захист від кінетичної зброї.

4. Автономна поведінка: системи контролю, орієнтовані на великі рої, та інтелектуальна автономія (тобто все більш вдосконалений вбудований ШІ), точна навігація, цифрове управління.

Автономність платформи є одним з найважливіших застосувань для робототехніки та автономних систем, що відносяться до військових питань [34]. Автономні системи з підтримкою штучного інтелекту (особливо невеликі) спровокували нові технологічні розробки та використання космосу. Відповідні дослідження охоплюють широкий спектр технологій, включаючи: стелс (сигнатури: інфрачервоний, акустичний); кваліфікацію та сертифікацію; конструкції та матеріали; двигуни; продуктивність; стабільність та керованість; дизайн;

5. Використання віртуальних програмних агентів або ботів щодо наступальних та захисних дій в інформаційному та кіберпросторі. Розроблення безпечних, надійних автономних програмних агентів як частини кіберфізичної імунної системи [35] забезпечить засобами протидії бот-мережам та атакам шкідливого ПЗ та інших кібератак. Програмне

забезпечення повинно для прийняття важливих рішень використовувати автономність, щоб знизити когнітивне навантаження на оператора.

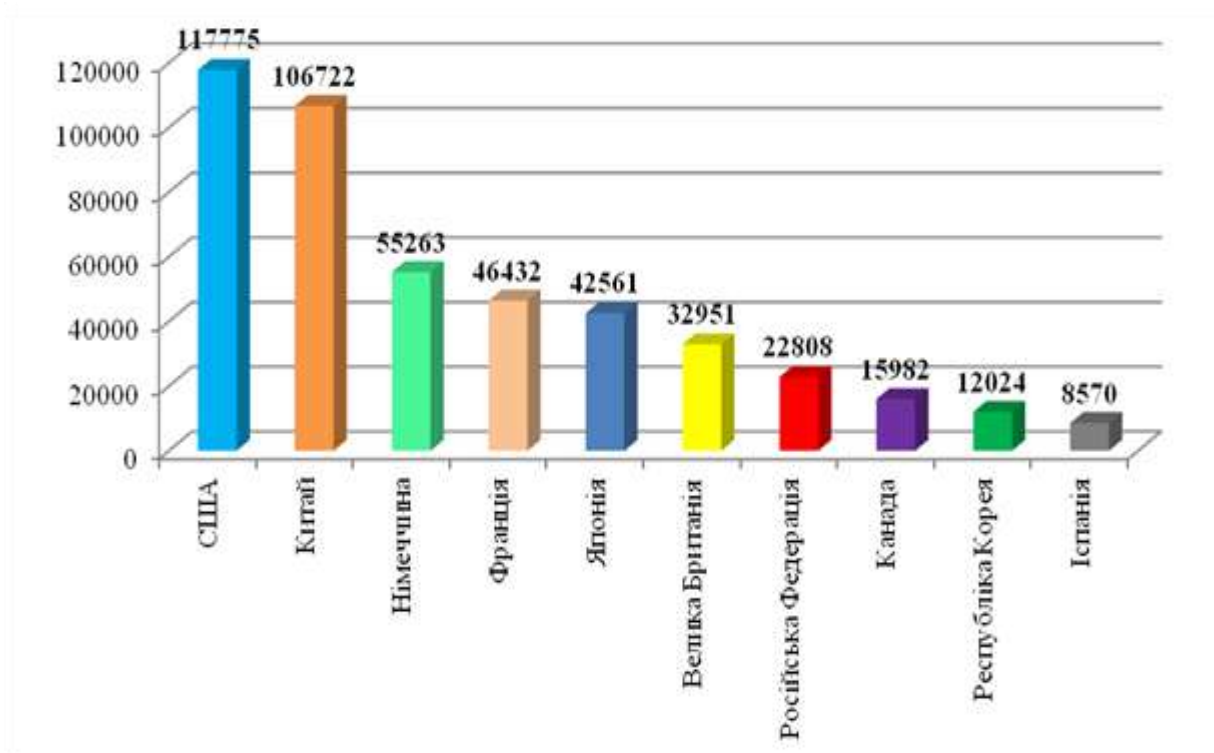
*Прогноз ринку.* Нова технологія безпілотників створила нову арену гонки озброєнь. До 2022 року очікувана ринкова вартість для військових БПЛА у всьому світі досягне 15 млрд дол. США.

Прогноз ринку військових роботів становить 30,8 млрд дол. США у 2022 р. [36].

Світові витрати на військову робототехніку у 2019 році перевищили 115 млрд дол., що на 17,6% вище, ніж у 2018 році. Зростання ринку буде обумовлено великими інвестиціями з боку США, Китаю, Росії та Ізраїлю в технології нового покоління, а також власними розробками і масштабними закупівлями цих технологій і технічних засобів на їх основі Індією, Саудівською Аравією, Південною Кореєю і Японією.

## КОСМІЧНІ ТЕХНОЛОГІЇ

Найвищий потенціал космічних технологій у військовій сфері мають США, Китай, Японія та країни ЄС (рис. 10).

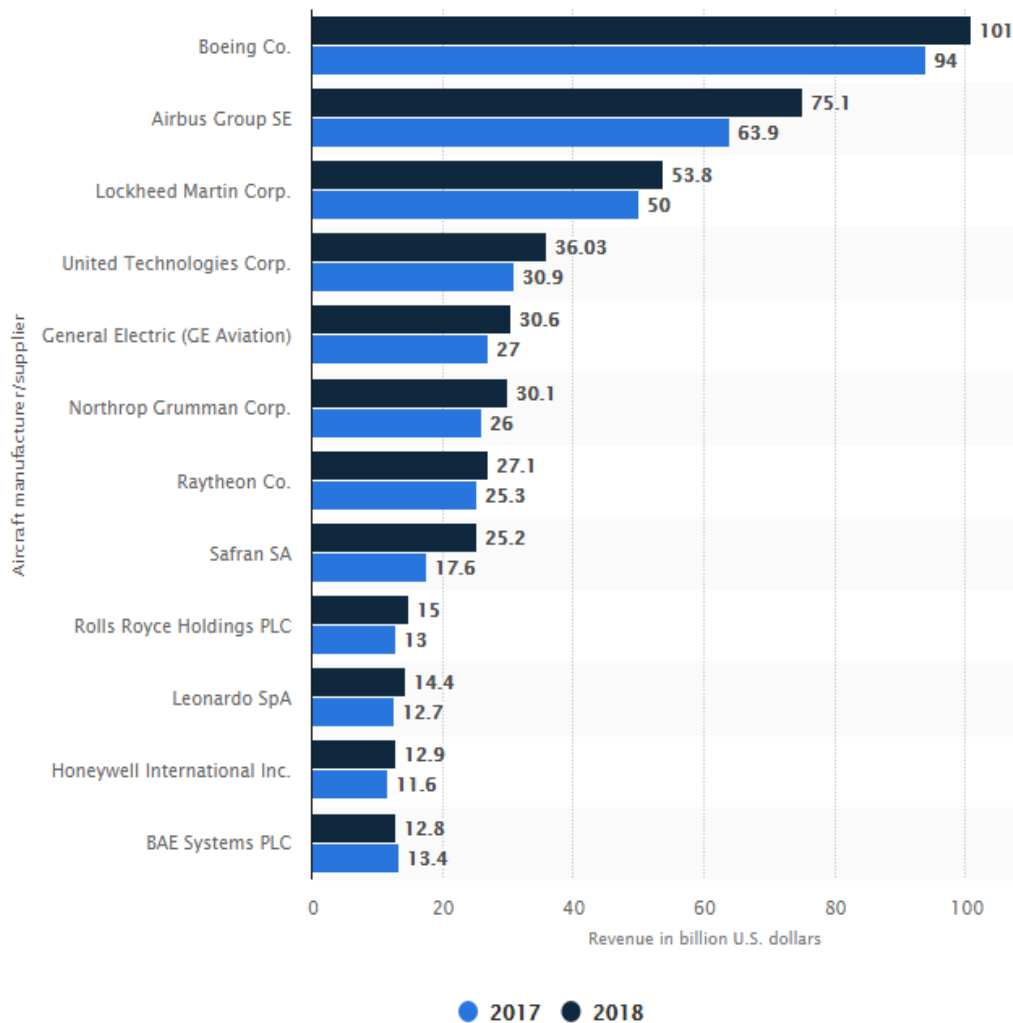


Джерело: Derwent innovation

**Рис. 10** Топ-10 країн світу за кількістю патентів у сфері військових космічних технологій, од.

Аерокосмічна та оборонна промисловість США забезпечує більшість міжнародного попиту на військові космічні технології та апаратуру. З точки зору міжнародного порівняння, багато провідних світових аерокосмічних виробників знаходяться в США – це шість з 11 провідних аерокосмічних компаній (рис. 11). Boeing Company, United Technologies та Lockheed Martin є трьома провідними компаніями-постачальниками оборонних технологій США за рейтингом на основі прибутків у 2018 році.



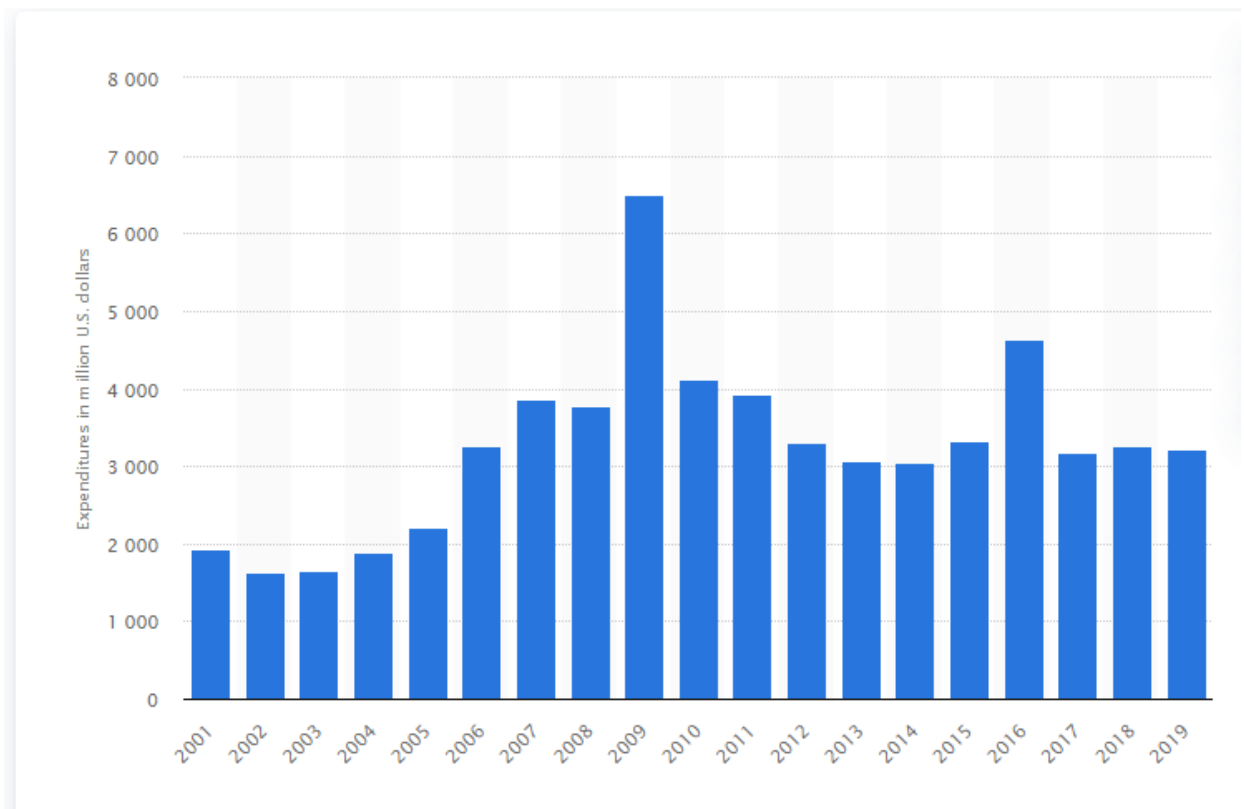


Джерело: Leading aircraft manufacturers and suppliers in 2017 and 2018, based on revenue. - <https://www.statista.com/statistics/268991/expenditures-on-research-and-development-by-boeing/>

**Рис. 11** Лідери світової аерокосмічної галузі за обсягами доходів у 2017-2018 рр., млрд дол. США

У 2018 році світовий дохід *Boeing* склав близько 101 мільярда доларів США. НДДКР – ключовий фактор в аерокосмічній галузі. Результати досліджень та розробок є життєво важливими в цій галузі.

Витрати на дослідження та розробки *Boeing* становили близько 3,2 млрд дол.в США у 2019 році порівняно з майже 3,3 млрд дол. США у 2018 році (рис. 12).



Джерело: Boeing's R&D expenditures from FY 2001 to FY 2019. - <https://www.statista.com/statistics/268991/expenditures-on-research-and-development-by-boeing/>

**Рис. 12** Витрати на наукові дослідження і розробки компанії Boeing у 2001-2019 рр., млрд дол. США

Зменшення витрат відбулося внаслідок зменшення витрат на моделі 737 та 777. Рівень витрат на дослідження та розробки був найвищим у 2016 році напередодні запуску реактивного сімейства 787 Dreamliner. Dreamliner – одна з найважливіших модельних сімей компанії, що відстає лише від серії 737.

Boeing постійно конкурує за замовлення з конкурентом *Airbus*. Без вкладень у нові інновації будь-яка компанія залишиться позаду. Boeing, як очікується, понесе додаткові витрати на дослідження та розробку для переробки літака 737. Це буде необхідно для дотримання нових стандартів безпеки, що виникли внаслідок проблем у моделі 737, які призвели до двох смертельних аварій у 2018 та 2019 роках.

*Lockheed Martin* є провідною компанією, що виробляє аерокосмічну техніку, забезпечує підтримку військової галузі та є найбільшим підрядником у галузі оборони у всьому світі. Компанія також є провідним світовим дилером зброї та виробником військової техніки.

Щоб зберегти свої лідируючі позиції, постачальник оборонних технологій Lockheed Martin послідовно інвестує у дослідження та розробки, у 2019 році відповідна сума становила приблизно 1,3 млрд дол. США. За останні

роки компанія пережила зростання, оскільки еволюціонували міжнародні конфлікти, а країни продовжують збільшувати свої військові витрати. Наприклад, з 2000 по 2019 рік дохід Lockheed Martin збільшився більш ніж удвічі – з 25 у 2000 р. до близько 60 млрд дол. США у 2019 р. З іншого боку, операційний прибуток компанії зріс майже у вісім разів за той самий період, досягнувши 8,5 млн дол. США у 2019 році. Це свідчить про актуальну модель зростання аерокосмічного та оборонного постачальника Lockheed Martin.

Технологічні тренди для військово-повітряних сил розглянуто у публікації 2019 р. [37].

У даній роботі розглянуто тільки нові тенденції, яким на сьогодні визнається космос як область ведення бойових дій [38].

Важливість космосу підтверджується діями військового командування найбільш розвинених у військовому плані країн.

У серпні 2019 р. у США створено Космічне командування США (SPACECOM) та Космічні сили США у складі 87 частин і підрозділів, в компетенції яких знаходяться оповіщення про ракетні загрози, управління космічними польотами і підтримка операцій в космосі. Цією ініціативою визнається зростаюче значення космосу як області ведення бойових дій.

У 2020 р. затверджено Стратегію оборони у космічному просторі (DSS) [39], якою визначається, як Міністерство оборони США розвиватиме космічні сили, щоб конкурувати, стримувати та перемагати в складних умовах безпеки. Необмежений доступ до космосу та свобода його експлуатації є життєво важливими для безпеки, процвітання та наукових досягнень США.

Космічна галузь *КНР* швидко розширює спостереження та розвідку (ISR), використовує супутники навігації та зв'язку та досягає значних успіхів у своїх можливостях запуску в космос, польотів людей у космос та дослідженнях Місяця. Китай розробив космічну ракету-носій "швидкого реагування" (SLV), щоб підвищити свою привабливість як комерційного постачальника невеликих супутників та можливостей їх запуску і використання у навколоземному космічному просторі.

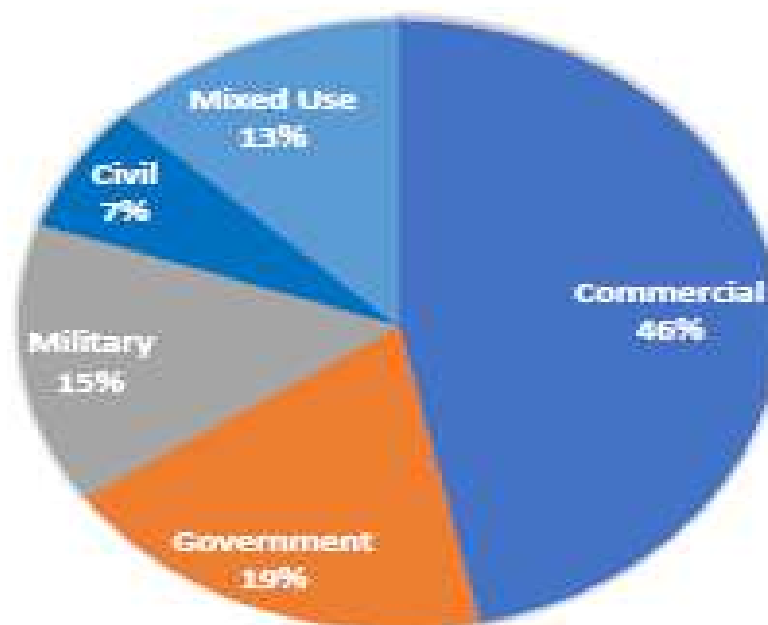
ВПС Франції 11 вересня 2020 р. перейменовані у французькі повітряно-космічні сили, чим завершився процес, ініційований президентом Еммануелем Макроном у липні 2019 року, коли він оголосив про створення космічного командування. У своїй заяві Повітряно-космічні сили зазначають, що, враховуючи "життєво важливе значення для військових операцій",

Франція визначила космос як "головний пакет акцій" для своєї стратегічної незалежності, і тому Космічне командування, відоме як CDE або Commandement de l'espace, було створено 3 вересня 2019 року.

Космічне командування повинно досягти повної оперативної спроможності у 2025 р. зі штатом майже 500 осіб. У даний час 220 чоловіків і жінок працюють над розвитком захисту військових супутників від наближення супутників, які експлуатуються іноземними державами. Франція вже створила лабораторію LISA для розроблення військових інновацій у космосі, а також готується до AstérX, перших європейських військових космічних навчань, запланованих на листопад 2020 року.

Для використання космосу як для мирних, так і військових дій потрібен національний або комерційний доступ до ракет-носіїв, платформ (супутників), датчиків, роботи та рої, стійкі до загрози навколишнього середовища або техногенного середовища. На сьогодні країни світу володіють 2666 супутниками, серед них 1327 належать США, Китаю – 363, Росії – 169.

Із зазначеної загальної кількості супутників 15% або 400 од. є військовими (рис. 13), з яких 192 належать США. Ще 346 супутників використовуються для різних цілей, у т.ч. і військових.



Джерело: [38]

**Рис.13 Розподіл супутників, які функціонують на орбіті Землі, за функціями**

На сьогодні наукові дослідження та розроблення технологій стосуються датчиків (стиснене зондування, комп'ютерне зображення, стійке інфрачервоне спостереження); матеріалів (зберігання енергії, 3D-друк) та операцій (система управління здоров'ям, тривимірне екологічне моделювання, лазери ультракоротких імпульсів, широкосмуговий зв'язок, робототехніка та автономія).

Технології космосу, які розвиваються сьогодні, розглянуто на прикладі США як основного їхнього автора та користувача. Дослідження США щодо космічних технологій стосуються [39]:

- Системи глобального позиціонування "NAVSTAR"
- Системи відслідковування погоди
- Системи інформування про космічну ситуацію
- Прототипу космічних систем
- Технологій космічного контролю
- Мережі супутників зв'язку для Космічних сил, які будуть використовуватися для захищеного зв'язку
- Полярної системи MILSATCOM (космічної)
- Системи відслідковування пусків ракет Next Generation OPIR
- Програми безпеки національної космічної системи
- Космічного випробувального і навчального полігону
- Програми запуску ракетних систем
- Програми космічних випробувань
- Системи космічних ліфтів
- РЛС балістичної протиракетної оборони
- Системи виявлення ядерної детонації (NUDET Detection System (SPACE)) тощо.

Наприклад, *Глобальна система позиціонування (GPS)* – це система космічного радіолокаційного позиціонування, навігації та хронометражу (PNT). Обладнання GPS (UE) складається зі стандартизованого приймача, антени, антенної електроніки та іншого супутнього обладнання, згрупованих в набори для отримання навігаційної та часової інформації, що передається від GPS-супутників. Дослідження, розробка, випробування та оцінка передбачається щодо інтеграції, тестування та аналізу нових можливостей приймача PNT на всіх військових платформах, що використовують служби GPS.

Програма із розроблення обладнання для військової глобальної системи позиціонування (MGUE) відповідає за розроблення стандартних

модернізованих приймачів для військових платформ. Документ про розвиток можливостей MGUE 2014 р. ініціює нове сімейство модернізованих приймачів GPS, що забезпечить значно покращену здатність протистояти негативним впливам і, тим самим, унеможливленню військових операцій.

Друга редакція програми (MGUE Inc 2 CDD затверджена 6 квітня 2018 року) продовжує роботи із вбудовування технологій військових приймачів в інші програми (космічні приймачі та прецизійні керовані боєприпаси). Програма MGUE Inc 2 виконується у трьох частинах: 1) діяльність зі зменшення ризиків, 2) швидке створення прототипу карти приймача з мініатюрним послідовним інтерфейсом (MSI) для середнього рівня, 3) спільний модернізований портативний прилад GPS для швидкого створення прототипу.

Стратегія включає два проєкти із швидкого прототипування середнього рівня: 1) приймальних карт з мініатюрним послідовним інтерфейсом (MSI), що включає інтегральну схему наступного покоління (ASIC), та 2) спільний модернізований портативний приймач.

*Програма технологій космічного контролю* передбачає заходи із системного проєктування, технологічного планування, демонстрації і прототипування тактики і процедур для оперативно реагуючої та стійкої роботи зони Space Control. Програма включає розроблення технологій і прототипів для оборонного контрпростору (DCS) та наступального контрпростору (OCS) і необхідну системну інженерію для військового винищувача для ефективного використання таких систем.

Зокрема підтримується діяльність DCS та космічної ситуаційної обізнаності (SSA), які включають розробку корисного навантаження попередження про загрози для моніторингу, виявлення, ідентифікації, відстеження, оцінки, перевірки, категоризації і визначення характеристик об'єктів та подій у космосі. Крім того, ця діяльність підтримує розробку прототипів корисного навантаження та комплектів сил космічної оборони для захисту космічних систем, ресурсів та операцій США від спроб ворога нейтралізувати їх, втрутитись або знищити.

Конкретні заходи OCS включають порушення, відмову або деградацію (та пов'язану з ними електронну підтримку) космічних систем противника, які можуть бути використані для визначених цілей, ворожих інтересам національної безпеки США. Розроблено можливості швидкого реагування у відповідь на негайні потреби військових винищувачів у зоні місії космічного контролю в рамках цієї програми.

*Драйвери росту космічних технологій:*

1. *Smallsats*: малі космічні апарати вагою менше 500 кг підтримують багато різних можливостей, оскільки можуть виконувати військові завдання, які колись виконували великі космічні кораблі. Сьогодні апарати різних розмірів та ступенів автономності вже використовуються для збору розвідувальної інформації (ISR), використовуючи дуже короткий час виконання завдань, швидкий запуск та гнучке позиціонування. Збільшення використання маленьких кораблів з новими пасивними та активними датчиками з низьким рівнем потужності збільшить ситуативну обізнаність стану навколо планети та підвищить розуміння ситуації в космосі. У майбутньому рої малих апаратів підвищать автономність та ще більше покращать можливості C4ISR.

2. *Мікрохвильова фотоніка*: може сильно вплинути на функціональні можливості та характеристики космосу для високочастотних радарів. Інтеграція фотоніки може допомогти зменшити розмір і вагу, а також збільшити стійкість до електромагнітних перешкод. Вже було продемонстровано, що інтегрована фотонна технологія відповідає військовим потребам у космосі.

3. *PCL*. Збільшення дальності виявлення наземних радарів з пасивною когерентною локацією (PCL), доповнене приймачами космічного базування, дозволить у реальному часі забезпечувати зйомку великих територій. Це дозволить глибше спостерігати за діяльністю на значній території і забезпечувати знаходження, відслідковування, та ідентифікацію цілей з використанням передатчиків противника або нейтральної сторони. Ця технологія дозволить також відслідковувати гіперзвукові запуски.

4. *Квантові технології*: одна із головних переваг квантових технологій буде реалізована в середньостроковій перспективі у програмах зондування, зокрема із виявлення затоплених або прихованих об'єктів. Покращена візуалізація за допомогою різних методів може забезпечити більш швидке та точне виявлення загроз. Квант потенційно може суттєво покращити безпечний зв'язок, але є кілька проблем, які потрібно вирішити щодо відстані та розміру мережі. Тим не менше, швидке виявлення вторгнення може бути суттєвою допомогою для кіберрозвідки.

5. *Терагерцові датчики*: підтримуватимуть екзоатмосферне зондування з високою роздільною здатністю, а потужності перехоплення і протидії цих технологій унеможливають використання супротивником їхнього потенціалу проти власника технології.

6. *Поінформованість про ситуацію* в космосі стане критичною. Збільшення обсягів космічного сміття, перевантаженість орбіт, наявність

великої кількості малих супутників і космічних апаратів-перехоплювачів, знання космічної погоди і т. д. вимагатимуть підвищення космічної ситуаційної обізнаності.

*Ризики та обмеження для космічних технологій:*

1. Smallsats: швидко падаючі ціни на космічні старты та зростаюча мініатюризація космічних кораблів збільшить доступ до космосу, у т.ч. для кримінальних елементів.

2. Мікрохвильова фотоніка: застосування мікрохвильової фотоніки в бездротових системах зв'язку та розподілених сенсорних мережах зробить цю технологію доступною у всьому світі. Це дозволить розробляти дедалі менші та більш функціональні супутники та рої.

3. PCL: супротивник може отримати можливість виявлення, відстеження і використання радарів і передатчиків користувача на основі нових технологій.

4. Терагерцові датчики: особливе занепокоєння викликає можливість легкого виявлення невидимих об'єктів, використовуючи космічні терагерцові датчики.

5. Ризики від протисупутникової зброї (ASAT) або роботизованих систем стануть більш загрозливими. Збільшення перевантаженості орбіт, збільшення використання великих роїв малих апаратів та збільшення космічного сміття впливатиме на ефективність та надійність космічних систем.

*Прогнозовані напрями наукових досліджень і розроблення технологій – це платформи, операції та сенсори, або більш детально:*

1. Мікрохвильова фотоніка.

2. Малі космічні кораблі: різноманітні малі кораблі вже використовуються в рамках військових операцій у всіх сферах. Однак ці системи обмежені у своєму використанні та можливостях. Передбачаються дослідження із збільшення рівня автономності, покращання супутникового управління, специфічного коригування орбіти відповідно до місії.

3. Автономія: розширення орбітальних автономних можливостей, тобто, розширення можливостей штучного інтелекту та обробки, покращення технологій накопичення енергії, ефективніші технології двигуна та вдосконалена робототехніка.

4. Радари пасивної когерентної локації.

5. Квантова заплутаність.

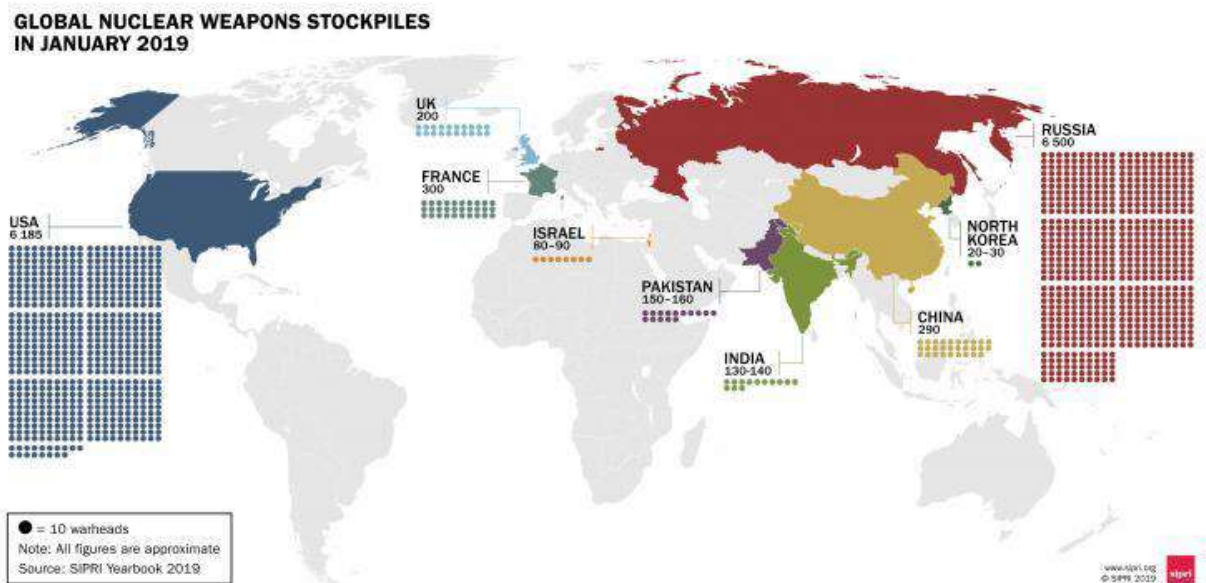
6. Датчики терагерцового діапазону.

7. Стійкість космічних активів і мереж.



## ЯДЕРНА ЗБРОЯ

У світі існує дев'ять ядерно-озброєних держав – США, Росія, Велика Британія, Франція, Китай, Індія, Пакистан, Ізраїль та Кореїська Народно-Демократична Республіка (Північна Корея) – разом мають приблизно 13 400 од. ядерного озброєння на початку 2020 р. Це означає зменшення порівняно з 13865 од. ядерного озброєння, яким, за оцінками СІПРІ, ці держави володіли на початок 2019 року. Найбільший арсенал має Росія – 6500 од., на другому місці – США із 6185 од. (рис. 14).



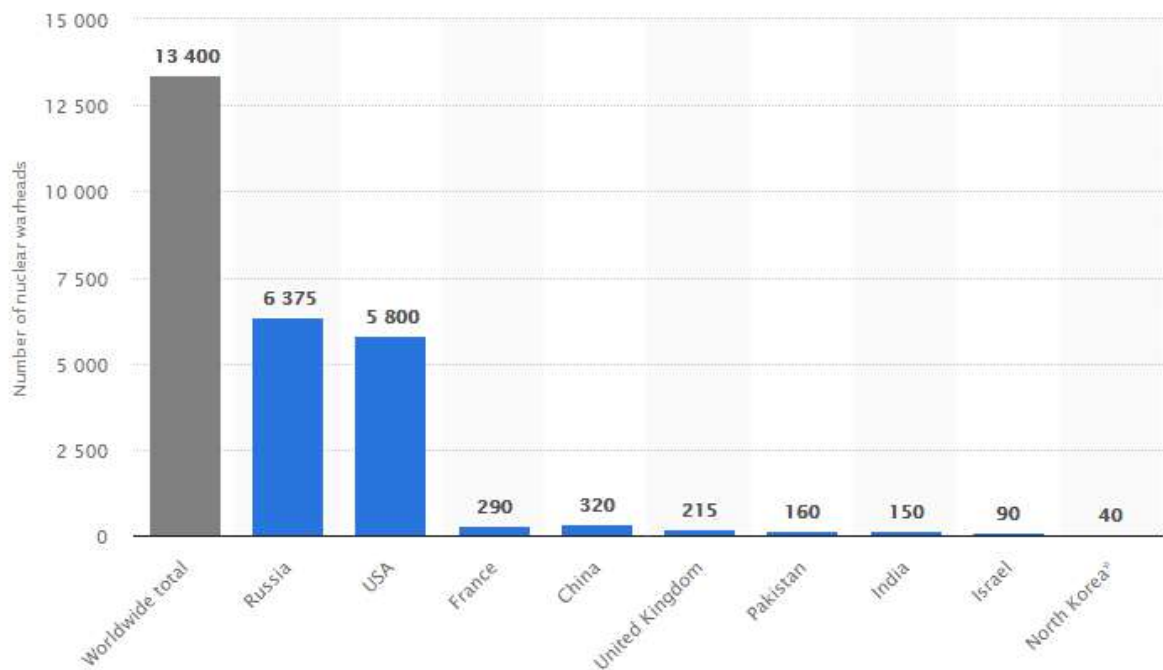
Джерело: [40]

**Рис. 14** Ядерний арсенал країн світу станом на кінець 2019 року

За даними STATISTA, розподіл ядерних боєголовок між країнами у світі трохи інший – Росії і США належить дещо менша кількість (6375 проти 6500 та 5800 проти 6185 од. відповідно), але Китаю – дещо більша – 320 од. проти 290 од. (рис. 15).

У даний час близько 3720 ядерних одиниць розгорнуто в оперативних силах, і майже 1800 з них перебувають у стані підвищеної оперативної готовності.

На піку гонки ядерних озброєнь холодної війни в 1986 році кількість ядерних боєголовок у всьому світі, за оцінками, становила майже 65000. Згідно з тим самим аналізом, у 2017 році було трохи більше 9000 активних боєголовок.



Джерело: Number of nuclear warheads worldwide as of January 2020. - <https://www.statista.com/statistics/264435/number-of-nuclear-warheads-worldwide/>

**Рис. 15** Розподіл ядерних боєголовок між країнами станом на січень 2020 року, од.

Зменшення загальної кількості ядерної зброї у світі у 2019-2020 роках значною мірою відбулося внаслідок демонтажу застарілої ядерної зброї Росією та США, які разом досі мають понад 90 % глобальної ядерної зброї. Скорочення американських та російських стратегічних ядерних сил, передбачене Договором 2010 року про заходи щодо подальшого скорочення та обмеження стратегічних наступальних озброєнь (Новий СНВ), було завершено у 2018 р., а у 2019 р. сили обох країн залишились нижче обумовлених договором меж. Новий СНВ втратить чинність у лютому 2021 року, якщо обидві сторони не домовляться про його продовження.

Однак дискусії щодо його продовження або переговорів щодо нового договору не просунулись з 2019 року. Це було частково пов'язано з наполяганням адміністрації США на тому, що Китай повинен приєднатися до будь-яких майбутніх переговорів про скорочення ядерної зброї, але Китай категорично відмовився зробити це.

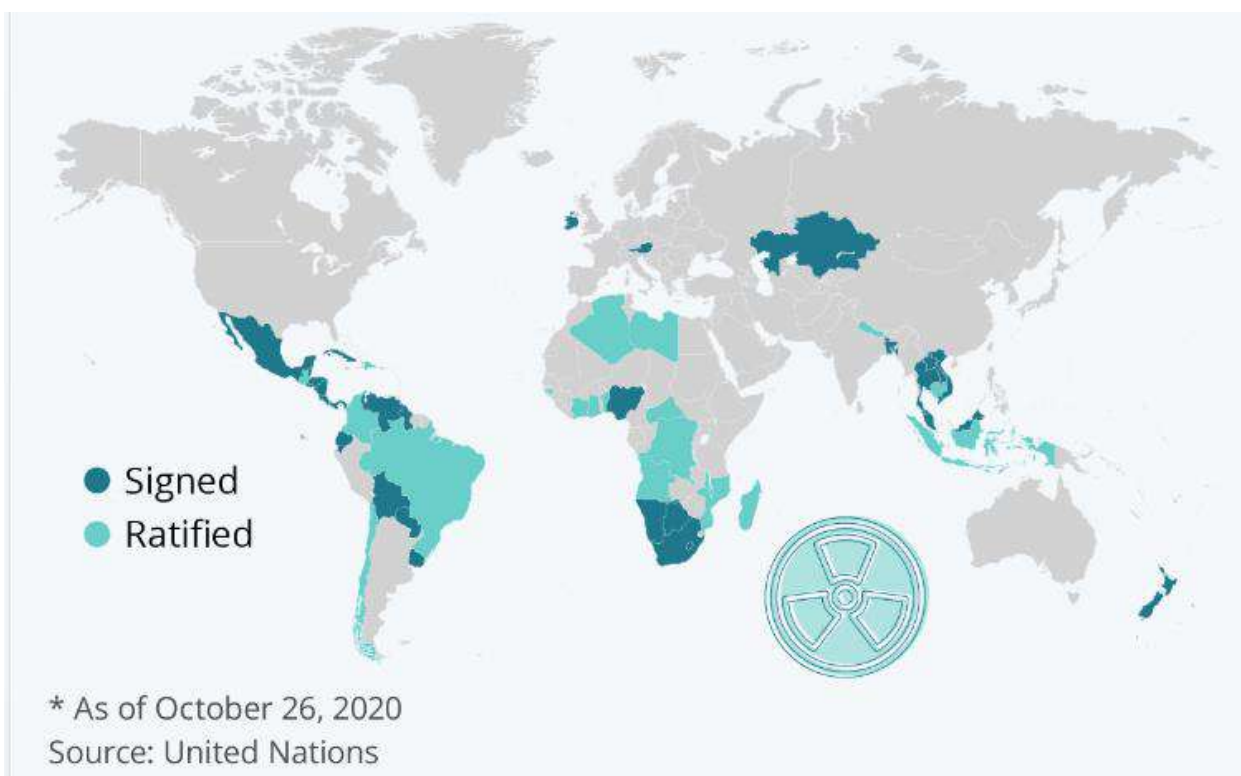
“Тупиковий шлях до нового СНВ та розвал радянсько-американського договору 1987 року про ліквідацію ракет середньої і меншої дальності у 2019 році свідчить про те, що ера двосторонніх угод про контроль над ядерною зброєю між Росією та США може добігати кінця“, – говорить Шеннон Кіл, директор програми ядерного роззброєння, контролю над озброєнням та

нерозповсюдженням SIPRI. “Втрата ключових каналів зв'язку між Росією та США потенційно може призвести до нової гонки ядерних озброєнь”.

В той же час, 26 жовтня 2020 р. Організація Об'єднаних Націй заявила, що її Договір про заборону ядерної зброї ратифікований 50-ю країною, що означає, що він набере чинності 22 січня 2021 року.

Договір про ядерну зброю, який забороняє використання, розробку, виробництво, випробування, розміщення, накопичення запасів і застосування такої зброї, був схвалений Генеральною асамблеєю ООН у липні 2017 року за погодженням 122 країн. Група ядерних держав, в тому числі США, Великобританія, Франція, Китай і Росія, не підписали договір. Тому договір про заборону ядерної зброї залишатиметься значною мірою символічним.

Гондурас став 50-ю країною (рис. 16), яка ратифікувала договір після того, як це зробила ціла низка країн після 75-ї річниці атомних вибухів у Хіросімі та Нагасакі.



Джерело: The Status Of The UN's Treaty Banning Nuclear Weapons. - <https://www.statista.com/chart/23288/status-of-un-treaty-banning-nuclear-weapons/>

**Рис. 16 Статус договору ООН про заборону ядерної зброї**

Наявність достовірної інформації про стан ядерних арсеналів та можливості ядерних озброєних держав значно варіюється. "США розкривали

важливу інформацію про свої запаси та ядерний потенціал, але в 2019 році адміністрація США припинила практику публічного розкриття розміру своїх запасів", – говорить Ганс М. Крістенсен, старший науковий співробітник відділу ядерного роззброєння, контролю над озброєнням Програми нерозповсюдження та директор проекту ядерної інформації при Федерації американських вчених (FAS). Велика Британія та Франція також оголосили певну інформацію. Росія не робить загальнодоступним детальний розподіл своїх сил, розрахованих за Новим СНВ, хоча вона ділиться цією інформацією зі США [40].

Ядерні арсенали інших ядерно-озброєних держав значно менші, але всі ці держави або розробляють, або застосовують нові системи озброєнь, або заявили про свій намір це зробити.

Уряди Індії та Пакистану роблять заяви щодо деяких своїх ракетних випробувань, але надають мало інформації про статус або розмір своїх арсеналів. Північна Корея визнала проведення випробувань ядерної зброї та ракет, але не надає інформації про свої можливості щодо ядерної зброї. Ізраїль проводить давню політику не коментувати свій ядерний арсенал.

Зараз відбувається постійне погіршення умов міжнародної стабільності. Ця тенденція відображається, серед іншого, в розгортанні кризи контролю над ядерним озброєнням, який зазнав подальших невдач у 2019 році. Нестабільний характер глобальної політики означає, що кількість сторін, що контролюють ядерні боєголовки, викликає більше занепокоєння, ніж кількість самих боєголовок.

Дві країни, що мають найбільші сучасні арсенали, також несуть найбільшу відповідальність за найбільшу кількість ядерних випробувань починаючи з початку випробувань у 1945 р. У період з 1945 по 2019 р. США провели 1030 ядерних випробувань. Відповідна кількість в Росії, включаючи СРСР, становить 715. Хоча Росія та США мають подібну кількість боєголовок, США щороку виділяють значно більший обсяг фінансових ресурсів для своєї ядерної програми.

Світове співтовариство з великим занепокоєнням спостерігає за ядерним розвитком Ірану та Північної Кореї. Індекс ядерної небезпеки оцінює ризик для Північної Кореї та Ірану найвищим серед країн, що мають ядерний потенціал. Незважаючи на увагу, Північна Корея продовжувала його нарощування і за останні п'ять років значно збільшила кількість випробувань балістичних ракет [41].

*Розробляються системи ядерної зброї наступного покоління.* Росія та США розробляють великі та дорогі програми із заміни та модернізації своїх ядерних боєголовок, систем доставки ракет і літаків, а також потужностей з

виробництва ядерної зброї. Обидві країни також бачать нову або розширену роль ядерній зброї у своїх військових планах та доктринах, що знаменує собою нову тенденцію щодо поступової маргіналізації ядерної зброї. США стверджує, що Росія розробила і розгорнула мобільну наземну крилату ракету, що має дальність польоту, заборонену договором.

Китай знаходиться у середині процесу значної модернізації свого ядерного арсеналу. Він вперше розробляє так звану ядерну тріаду, що складається з нових ракет наземного та морського базування та літаків, здатних нести ядерну зброю. Індія та Пакистан повільно збільшують масштаби та різноманітність своїх ядерних сил, тоді як Північна Корея продовжує надавати пріоритет своїй військовій ядерній програмі як центральному елементу стратегії національної безпеки. Хоча Північна Корея дотримувалась самопроголошеного мораторію на випробування ядерної зброї та балістичних ракет великої дальності у 2019 році, протягом року вона провела багаторазові льотні випробування балістичних ракет меншої дальності, включаючи кілька нових типів систем.

Бюджетний запит Міністерства оборони США на 2021 р. містить пункти щодо *модернізації ядерної зброї* шляхом інвестування у наукові дослідження і розробки з розроблення нового покоління платформ доставки та закупівлі систем доставки ядерної зброї, таких як існуючий Trident II, балістичних ракет наземного стратегічного стримування (GBSD), B61 -12 Tail Kit, а також програм зброї Long Range Standoff (LRSO), які замінять повітряну крилату ракету (ALCM) після закінчення терміну її служби.

*Для військово-морських сил* запит передбачає фінансування двох атомних авіаносців класу FORD: CVN-80 та CVN-81 та їхнє науково-технічне супроводження. Бюджетний запит також включає: наукове забезпечення будівництва підводного човна класу Колумбія із балістичними ракетами та атомного авіаносця нової конструкції і заправного комплексу для авіаносців. Також передбачається фінансування наукових досліджень і виробництва:

- Trident II (D5) – балістичної ракети, яка запускається з підводного човна. Trident II забезпечує можливість нанесення другого удару (у відповідь) в ядерній триаді країни;
- атомних підводних човнів класу «Вірджинія» і «Колумбія»;
- авіаносця класу CVN 78 з новим реактором A1B і розширеними можливостями зі зменшеним комплектуванням: електромагнітною системою старту літаків (EMALS), вдосконаленим пристроєм для затримання (AAG) та дводіапазонним радаром (DBR). Системи та конфігурація корабля

оптимізовані для максимізації кількості бойових вильотів (SGR) ударних літаків винищувачів за одиницю часу;

- програми продовження терміну експлуатації заправного комплексу CVN (RCOH), який призначений для обслуговування атомних авіаносців флоту.

*Для військово-повітряних сил* виділяються кошти на:

- B-21 Raider – перспективний високотехнологічний малопомітний стратегічний бомбардувальник;

- B-2 Spirit – багатомоторний бомбардувальник великої дальності, здатний нести звичайне і ядерне озброєння;

- Stratofortress B-52H – стратегічний бомбардувальник, який може нести ядерні та звичайні бомби, ракети;

- тактичний ракетний комплекс з гіперзвуковими плануючими боєприпасами, який розробляється у рамках проекту OpFires. Розроблення такого ракетного комплексу почалося у США у 2019 р., передбачається, що випробування розпочнуться у 2023 році.

*Для наземних сил* передбачається фінансування наукових досліджень і закупівель:

- Stryker – 19-тонний колісний броньований автомобіль, який забезпечує армію сімейством з 24 різних платформ. Існує дві базові версії: для піхоти (ICV) та для мобільної гарматної системи (MGS) у восьми модифікаціях, у т.ч. для протитанкових керованих ракет і ядерного, біологічного, хімічного та радіологічного озброєння;

- програми наземного стратегічного стримування (GBSD) із заміни застарілої міжконтинентальної балістичної ракети новою, яка повинна бути на озброєнні до 2075 року. Ця система є частиною ядерної тріади;

- LRSO – крилата ракета повітряного базування, може використовуватися в середовищах без GPS, яка замінить ракети ALCM AGM-86, які почали експлуатуватися у 1982 році і вже значно перевищили свій початковий 10-річний термін експлуатації;

- системи зв'язку SATCOM у трьох можливих варіантах: стратегічний для систем командування, управління і зв'язку ядерної компоненти збройних сил (NC3); для забезпечення тактичних комунікацій у суперечливих умовах; і ширококутовий / вузькокутовий для забезпечення великої пропускної здатності в менш суперечливих умовах.

Більшість ракетних програм *Китаю*, включаючи балістичні та крилаті ракетні системи, за якістю порівнянні з іншими міжнародними виробниками вищого рівня. Китай виробляє широкий спектр ракет – балістичних, крилатих, повітря-повітря і земля-повітря – для внутрішнього застосування та на експорт, і продовжує розширювати свої випробувальні установки. КНР публічно дебютувала з новим гіперзвуковим плануючим боєприпасом з ракетним двигуном під час параду до 70-ї річниці в жовтні 2019 року.

Військові вважають, що гіперзвукові планери і ракети зможуть долати системи протиповітряної і протиракетної оборони противника і наносити по його об'єктах високоточні удари [42].

Також у 2019 році Китай випробував і розгорнув вдосконалені системи S-400 SAM, які отримав від Росії у 2018 році. У 2018 році Китай наголосив на розробці своєї першої великої дальності ракети повітря-повітря (AAM).

## ТЕХНОЛОГІЧНА МОДЕРНІЗАЦІЯ ЗБРОЙНИХ СИЛ США

У 2014 році міністерством оборони США був ініційований комплекс заходів з розвитку збройних сил, який отримав назву «Defense Innovation Initiative (DII)».

Основною метою цієї ініціативи є виявлення унікальних шляхів (напрямів) підтримання технологічної переваги збройних сил США у XXI столітті і формування системи їх стійкого фінансового забезпечення. Ініціатива DII передбачає проведення великого комплексу робіт за напрямами:

- довгострокові дослідження і розробки, орієнтовані на виявлення перспективних напрямів створення нових зразків озброєння, військової і спеціальної техніки, які радикально змінять ситуацію в області технічного оснащення збройних сил. Тобто новизна технологій та створених на їх основі технічних засобів має обнулити (в американській трактуванні – компенсувати) ті досягнення, на які ймовірними противниками витрачено і витрачаються величезні кошти. Такими визначені: космічні технології; підводні технології; технології проведення винищувальних операцій і забезпечення переваги у повітрі; технології протиповітряної і протиракетної оборони (ППО і ПРО);

- вдосконалення комплексного (міжвидового) планування прикладних досліджень і технологічних розробок;

- забезпечення світового лідерства в інноваціях для оборонних потреб, що передбачає сприяння розвитку наукового співтовариства, що займається роботами в інтересах оборони, підготовку кваліфікованих кадрів для оборонної системи планування, придбання та управління життєвим циклом ВВСТ, а також стимулювання припливу молодих фахівців;

- розвиток підходів до проведення військових навчань і командно-штабних тренувань, що забезпечують скорочення термінів апробації інноваційних технологій;

- виявлення, адаптація та впровадження ефективних бізнес-моделей у процесі програмно-цільового планування, розробок і закупівель. Робота в цьому напрямку пояснюється тим, що швидкість насичення військ нововведеннями іноді гальмується неповороткістю існуючих систем управління розробкою та реалізацією програм розвитку збройних сил і озброєнь.



Усі п'ять напрямів пов'язані і націлені на інтенсивну технічну і технологічну гонку щодо підвищення ефективності системи озброєння, парирування можливості противника здійснити технологічний відрив, змусити його економічно знесилитися, наздоганяючи США або вишукуючи способи ліквідації нових загроз, і т. д. Отже, основна мета реалізації цієї стратегії – беззастережне досягнення військового успіху у всіх сферах збройної боротьби (в космосі, повітрі, на суші, на морі і в кіберпросторі).

Реалізація Національної оборонної стратегії (NDS) [43], затвердженої у 2018 р., протягом липня 2019 р. – червня 2020 р відбувалася за трьома пріоритетами (відповідно до звіту міністра оборони США [44]):

- посилення боєздатності та готовності військ;
- зміцнення союзників і побудова партнерських відносин;
- реформування міністерства оборони для підвищення ефективності та підзвітності [43].

Для досягнення цих пріоритетів було сформульовано 10 цілей, які частково вже виконані, частково будуть виконані до кінця 2020 р.:

1. Моніторинг і врахування всіх планів Китаю та Росії.
2. Впровадження концепції негайного реагування, реагування на непередбачувані події і динамічного використання збройних сил.
3. Перерозподіл та передислокація сил відповідно до NDS.
4. Досягнення більш високого рівня готовності.
5. Розроблення злагодженого плану зміцнення союзників та пошуку партнерів.
6. Реформування міністерства оборони.
7. Зосередження уваги на Китаї.
8. Модернізація збройних сил – інвестиції у революційні технології.
9. Розроблення реалістичних спільних військових ігор, навчання та навчальних планів.
10. Розроблення сучасної військової концепції ведення спільних бойових дій, і, зрештою, доктрини.

*Модернізація збройних сил* відбулася, зокрема, завдяки переходу від застарілих збройних сил до більш боєздатних сил майбутнього. Це дозволить підтримувати перевагу США на полі бою, що як ніколи важливо, оскільки Китай і Росія продовжують модернізувати свої збройні сили і домагатися переваг у нових технологіях, таких як штучний інтелект і 5G.

На виконання Національної оборонної стратегії Міністерство оборони розробило Стратегію модернізації армії США [45], яка зосереджена навколо єдиної цілі – підвищення боєздатності кожного солдату та кожної одиниці техніки. Стратегія модернізації армії (AMS) планує об'єднання всіх збройних сил (регулярна армія, національна гвардія, армійський резерв та армійські цивільні особи) до 2035 року у багатодоменні сили під єдиним командуванням Army Futures Command (AFC) для виконання головного завдання – захисту США і збереження їхніх позицій у якості домінуючої у світі сухопутної держави. AFC очолить вісім крос-функціональних команд (CFT) [46].

Ця стратегія фокусується на шести пріоритетах: системи високоточного озброєння великої відстані, бойові машини нового покоління, перспективний літальний апарат з вертикальним зльотом, армійська мережа (мережеве управління, контроль, зв'язок та розвідка: навігація із гарантованим визначенням положення у реальному часі), протиповітряна і протиракетна оборона та боєздатність збройних сил (боєздатність піхотинців, синтетичне тренувальне середовище).

Ці пріоритети розподіляються на 31 напрям модернізації AFC на основі впровадження сучасного озброєння і платформ з технологіями наступного покоління та три інших напрями, необхідних для майбутніх наземних бойових операцій:

- *Гіперзвук*: прискорена розробка гіперзвукової зброї, початок експлуатації якої заплановано на 2023 рік. У найближчі п'ять років заплановано понад 40 випробувань. Недавній тест Common Hypersonic Glide Body продемонстрував готовність цієї зброї уразити ціль після подолання 2000 миль менш ніж за 20 хвилин, досягаючи максимальної швидкості, яка у 17 разів перевищує швидкість звуку.

DARPA і ВВС США 02.09.2020 р. оголосили про успішне завершення випробувань двох варіантів концепції гіперзвукової повітряно-реактивної зброї (HAWC), під час яких прототипи були закріплені на фюзеляжі літака-носія. DARPA готово приступити до перших випробувань в умовах вільного польоту протягом календарного року.

У рамках програми, відомої як HAWC, створюється гіперзвукова ракета повітряного базування. У даний час в США розробляються кілька гіперзвукових ракет.

- *Мобільна зброя направленої енергії* у рамках місії ППО «Маневр ближньої дії» (M-SHORAD). Прототип системи – це 50 кіловатних лазерів, встановлених на автомобілях Stryker. M-SHORAD забезпечить захист від

повітряних загроз – безпілотних апаратів і систем, ракет, артилерії, мінометів.

- *Мобільна наземна система озброєння, призначена для захисту від БПЛА і крилатих ракет.*

Бюджетний запит на 2021 фінансовий рік направлений на наукові розробки технологій, що забезпечать досягнення шести пріоритетів модернізації армії, зокрема:

- модернізацію Bradley, Stryker, Abrams і Paladin;
- систем M-SHORAD;
- наземних гіперзвукових ракет, ударних розвідувальних літаків майбутнього (FARA) і технологій використання низької навколоземної орбіти (LEO).

Бюджетні інвестиції в науку і технології (S&T) (у розмірі 2588 млн. доларів – найбільший в історії бюджет) поряд із науковим забезпеченням пріоритетів модернізації армії, направляються і на пошукові дослідження із забезпечення технологічної переваги США та запобігання непередбачуваних атак. Зокрема, фундаментальні дослідження повинні відкривати нові горизонти фундаментальної науки і техніки, керуючись довгостроковими можливостями із зміни правил гри. Прикладні дослідження повинні розробляти та оцінювати сучасні технології для потенційного військового застосування. Розвиток технологій (Advanced Technology Development) демонструє відпрацьовані технології, які можуть бути придбані найближчим часом.

Крім того, запит на 2021 фінансовий рік включає 46 мільйонів доларів на програмне забезпечення та цифрові технології. Ця пілотна програма Міністерства оборони направлена на оптимізацію розроблення і придбання програмного забезпечення для оборонних кібероперацій (для розроблення, закупівель, розгортання, модифікації і постійного вдосконалення програмного забезпечення). Цей пілотний механізм фінансування має на меті усунути проблеми, з якими стикаються керівники програм, намагаючись застосувати сучасні методи розробки програмного забезпечення.

Так, бюджет 2021 року підтримує такі кращі науково-дослідні ініціативи:

- *Штучний інтелект*: прискорене масштабування можливостей ШІ для потреб військ через Об'єднаний центр штучного інтелекту (JAIC). Розроблені перші в історії Принципи етики ШІ для того, щоб США були світовим

лідером у сфері розроблення та використання ШІ. JAIC пришвидшить інтеграцію можливостей ШІ в усі військові сфери шляхом подолання політичних, технічних та фінансових перешкод, а також за рахунок використання можливостей Мережі оборонних інформаційних систем (DISN).

- *Мікроелектроніка / 5G*: прискорення доступу США до передової комерційної та спеціальної мікроелектроніки, планується скористатися наявними можливостями 5G, не дозволяючи зловмисникам використовувати їх проти США. У рамках цих зусиль ініційовано великомасштабні експерименти з тестування та оцінки 5G можливостей зв'язку на 12 базах Міністерства оборони та галузевих партнерів.

- *Кіберкомандування*: кіберкомандування США (CYBERCOM) підтримує стратегію DoD, яка гарантує постійну взаємодію з кібер-акторами, підвищення спроможності бойового командування та підтримку урядових зусиль із забезпечення кібербезпеки.

- *Зусилля Advanced DoD із цифрової модернізації* хмарної IT-архітектури; ШІ; системи командування, управління і зв'язку; кібербезпеки.

Міністерство також рекапіталізує *стратегічну ядерну триаду* і ядерне командування, систему контролю і зв'язку (NC3) як вищий пріоритет. США домоглися великих успіхів у забезпеченні міцності і надійності засобів ядерного стримування країни. За останній рік було прийнято на озброєння нову малої потужності боєголовку балістичної ракети W76-2, що запускається з підводного човна. Також були розроблені і проведені експериментальні випробування дослідних версій двох видів традиційної ударної зброї середньої дальності з неядерною (конвенційною) бойовою частиною менш ніж за 12 місяців після того, як США вийшли з Договору про ракети середньої і малої дальності через неодноразові порушення угод Росією. У той же час розробляються системи захисту від перехоплювачів і балістичних ракет нового покоління, системи, що не відстають від ракетних систем противника і забезпечують багаторівневий захист країни.

Серед інших зусиль з *модернізації* – це проведення всебічного аналізу майбутнього *військово-морського флоту*. Планується розширити склад флоту до не менше ніж 355 кораблів, які включатимуть надводні бойові одиниці, великі підводні сили і, необов'язково, автономні судна, які забезпечать збереження панування США у відкритому морі.

У сфері *авіаційного озброєння* і військової техніки одним з перспективних напрямів розвитку є *розвиток безпілотних літальних*

*апаратів (БПЛА).* При їх виробництві широко використовуються високотехнологічні матеріали і сплави, застосовуються передові розробки в галузі двигунобудування.

Важливе місце займає оснащення безпілотних літальних апаратів електронно-обчислювальними системами бойового управління, навігації та зв'язку, що підвищує рівень бойової ефективності БПЛА. Наступним етапом вдосконалення цих апаратів є оснащення їх системами управління на основі штучного інтелекту.

Сполучені Штати прагнуть розширити області застосування БПЛА (розвідувальні, ударні, розвідувально-ударні, багатоцільові), збільшити їх номенклатуру і підвищити бойові можливості.

Одним із напрямів розвитку військової безпілотної авіаційної техніки є *зниження її залежності від людського фактору, підвищення автономності функціонування.* У зв'язку з цим військове керівництво США розглядає використання штучного інтелекту (в тому числі побудованого на застосуванні нейромереж) в якості одного з основних способів підвищення бойової ефективності БПЛА, а саме навчити БПЛА виконувати завдання, які традиційно вважаються прерогативою людини. За задумом, БПЛА повинні гнучко, майже "творчо", вирішувати поставлені завдання з урахуванням накопиченого "досвіду", правильно інтерпретувати вихідні дані і, використовуючи функції самонавчання і аналізу, "самостійно" приймати рішення щодо способу досягнення цілей. При цьому на сучасному етапі передбачається участь людини в контролі за діяльністю ШІ.

В якості основних областей застосування штучного інтелекту в БПЛА розглядаються аналіз і оцінка обстановки, а також розвідка, спостереження і розпізнавання (Intelligence, Surveillance and Reconnaissance – ISR).

У перспективі США планують об'єднати БПЛА з "інтелектуальними" обчислювальними системами на основі ШІ, які будуть працювати з великими базами даних (Big data). Наприклад, в якості основи для таких баз даних будуть використовуватися соціальні мережі (Фейсбук, Твіттер, Інстаграм) і інтернет-блоги. Крім того, розробляється програмне забезпечення, що імітує поведінку людини в соціальних мережах, з метою виявлення потенційно небезпечних суб'єктів, таких як представники терористичних та злочинних організацій.

Отримана інформація буде оброблятися спеціальними алгоритмами ШІ, а результати автоматично направлятися на БПЛА, які будуть самостійно приймати рішення щодо проведення тих чи інших заходів щодо обраної мети (в тому числі знищення). На особливу увагу заслуговує той факт, що однією з

бажаних характеристик системи є гнучкість, обумовлена алгоритмами навчання, щоб забезпечити можливість зміни категорій цілей і перерозподілу завдань по ним для використання в системі внутрішньої безпеки [47].

Міністр оборони Марк Еспер 09.09.2020 р. оголосив, що Пентагон має намір проводити випробування в реальному часі з тактичними літаками, керованими штучним інтелектом, у 2024 році.

Крім того, у серпні 2019 р. створено Космічне командування США (SPACECOM) та Космічні сили США у складі 87 частин і підрозділів, в компетенції яких знаходяться оповіщення про ракетні загрози, супутникові операції, управління космічними польотами і підтримка операцій в космосі.

Цією ініціативою визнається зростаюче значення космосу як області ведення бойових дій.

У 2020 р. затверджено *Стратегію оборони у космічному просторі* (DSS) [39], якою визначається, як Міністерство оборони розвиватиме космічні сили, щоб конкурувати, стримувати та перемагати у сучасних умовах.

Необмежений доступ до космосу є життєво важливим для безпеки, процвітання та наукових досягнень США. Наявність космічних можливостей є фундаментальною для встановлення та підтримання військової переваги в усіх сферах, а також для підвищення безпеки та економічного процвітання США і світової економіки. Стратегія була розроблена у відповідь на "загрозу з боку Росії і Китаю". Китай та Росія, які розглядають доступ до космосу як важливу складову своїх національних та військових стратегій, представляють найближчі та найсерйозніші загрози для космічних операцій США, хоча загрози з боку Північної Кореї та Ірану також зростають. Їхнє використання космічного простору значно розширюється.

DSS ініціює створення Космічних сил США, Космічного командування США та Агентства з космічного розвитку. Стратегія представляє космічні війська як унікальний рід збройних сил, який разом з іншими родами підтримує багатодоменні спільні та комбіновані операції з метою захисту національної безпеки.

Стратегія визначає 4 пріоритетні напрями зусиль для досягнення поставлених цілей:

- Створення всеосяжної військової переваги у космосі.
- Інтеграція військової космічної міці у національні, спільні операції.
- Формування стратегічного середовища.

- Співробітництво із союзниками, партнерами, представниками галузей та іншими урядовими агентствами і відомствами США.

Міністерство оборони передбачає використовувати готові комерційні технології та залучати економічно вигідні інвестиції, розширяти спільні дослідження і розробки (RD&A) із союзниками.

Орбітальне угруповання Міноборони США вже зараз має на озброєнні 130 космічних апаратів. Більше 40 супутників декількох типів використовується в складі глобальної системи зв'язку, що забезпечує обмін даними і управління військами по всій планеті. У складі навігаційної системи GPS використовується 31 супутник. Завдання розвідки вирішують 40 апаратів. Радіотехнічну, радіолокаційну і оптичну розвідку ведуть ще 15 апаратів. Шість супутників двох типів відповідають за відстеження космічних об'єктів. У системі попередження про ракетний напад задіяно 7 апаратів двох типів. Здійснюється взаємодія космічного командування і організацій з національної розвідки. Ведеться контроль над гіперзвуковою зброєю, ці завдання можуть вирішуватися супутниками попередження про ракетний напад. Ведеться створення нових навігаційних систем до вже існуючих GPS. Повідомляється про розробку *нової орбітальної зброї* для космічних сил США, в тому числі про *лазерні установки* [48].

У бюджетному запиті Міністерства оборони США на 2021 р. передбачаються кошти на програму лазерної енергії (High Energy Laser Research) у фундаментальних дослідженнях на суму у 15,1 млн дол. США [49] (Додаток А).

Також сповіщається, що США висунули програму колонізації Луни, на орбіту виводяться супутники Starlink, які дозволяють армії США з будь-якої точки земної кулі підтримувати зв'язок безпосередньо з Пентагоном і військовими базами. Білий дім пропонує у бюджеті 2021 р. на 12% збільшити фінансування НАСА з урахуванням пілотованого польоту на Луну до 2024 р. Крім того, на 19% зросте фінансування Національної адміністрації з ядерної безпеки.

Бюджетний запит Міністерства оборони США на 2021 фінансовий рік для *повітряних сил країни* передбачає фінансування:

фундаментальних досліджень на суму \$492,3 млн;

прикладних досліджень – \$1409,7 млн;

технологічних розробок – \$778,5 млн;

компонентних розробок та прототипів – \$7737,9 млн;

розвиток операційних систем – \$21466,7 млн. і т. д.

*Найбільші обсяги коштів* передбачені для таких досліджень:

- Прикладні дослідження: аерокосмічні двигуни – \$349,2 млн; аерокосмічні сенсори – \$211,3 млн; інформаційні науки та методи – \$178,7 млн.
- Технологічні розробки: демонстрація графічних ефектів – \$215,8 млн; платформа наступного покоління графіки – \$199,6 млн.
- Компонентні розробки і прототипи: програма розроблення стратегічного бомбардувальника-невидимки дальньої дії, спроможного доставляти термоядерну зброю – \$2828,4 млн; Ground Based Strategic Deterrent – система міжконтинентальних балістичних ракет наземного базування, що призначена для заміни всіх 450 ракет Minuteman III, які знаходяться на озброєнні ВПС США, починаючи з 2027 року – \$1524,8 млн; перспективний винищувач нового покоління за програмою Next Generation Air Dominace (NGAD) – \$1044,1 млн (можливі технології програмного забезпечення, plug-and-play, цифрової інженерії).
- Розвиток операційних систем і поставка: крилата ракета великої дальності – \$474,4 млн; RQ-4 Global Hawk – стратегічний розвідувальний безпілотний літальний апарат – \$134,6 млн; авіаційна система попередження і контролю – \$138,3 млн; F-22 A squadrons – тактична ескадрилья – \$665,0 млн; винищувач F-35 Joint Strike Fighter – \$785,3 млн і т.д.

Наукова програма в галузі космічних технологій [50], на яку передбачається виділення у 2021 р. 10,3 млрд дол. США, зосереджена на чотирьох основних сферах.

- 1) технології із розуміння космічної погоди та геофізичного середовища для використання цих знань у системах космічних сил;
- 2) технології експлуатації супутникового обладнання;
- 3) технології захисту космічних активів США у потенційних ворожих умовах;
- 4) технології космічних платформ та технології управління і взаємодії.

Управління перспективних дослідницьких проєктів Міністерства оборони США *DARPA* [51] сьогодні фокусує свої стратегічні інвестиції на чотирьох основних напрямках:

- 1) переосмислення складних військових систем: пришвидшення розвитку та інтеграції проривних військових можливостей у сучасний стрімко мінливий ландшафт, перетворення систем озброєнь у більш модульні системи, легша модернізація і вдосконалення; забезпечення переваг у повітряній, морській, наземній, космічній та кібер-сферах; покращення



навігації та хронометражу (PNT) не залежно від супутникової системи глобального позиціонування; та посилення захисту від тероризму;

2) інформаційний вибух: DARPA розробляє нові підходи до використання великих наборів даних за допомогою потужних інструментів великих даних. Агентство також розробляє технології надійності даних та систем, за допомогою яких приймаються важливі рішення, такі як автоматизовані можливості кіберзахисту та методи створення більш безпечних систем. Також приділяється увага зростаючій потребі у забезпеченні конфіденційності на різних рівнях потреби;

3) біотехнологія: для використання останніх проривів у галузі неврології, імунології, генетики та суміжних областях, DARPA у 2014 році створила бюро біологічних технологій, робота якого у цій галузі включає програми із прискорення прогресу в синтетичній біології, випередження поширення інфекційних хвороб та освоєння нових нейротехнологій;

4) розширення технологічної межі: DARPA працює над досягненням нових можливостей, застосовуючи сучасну математику; нові хімічні речовини, процеси та матеріали; квантову фізику.

Відповідно до національної політики та Директив Міністерства оборони, DARPA повністю підтримує безкоштовний науковий обмін та розповсюдження основних результатів досліджень у максимально можливих межах.

## ВИСНОВКИ

Сьогодні зони дій конфліктів поширилися на нові сфери, такі, як кіберпростір і космос. Начальник розвідувального управління Міністерства оборони Великої Британії генерал-лейтенант Джим Хокенхалл сказав: “Незважаючи на те, що традиційні загрози залишаються, ми спостерігаємо, як наші супротивники інвестують у штучний інтелект, машинне навчання та інші новаторські технології, водночас застосовуючи традиційні методи і важелі впливу”.

За словами генерала сера Річард Барронс, колишнього командувача Об'єднаного командування сил (Велика Британія): “Той самий широкий діапазон технології Четвертої промислової революції (обробка даних, зв'язок, штучний інтелект, робототехніка, біологічні науки, автономія тощо), що змінює спосіб нашого життя, роботу та ігри, змінить спосіб ведення війни. ... Військова трансформація здебільшого стосуватиметься швидкого впровадження та адаптації технологій та методів, що походять із цивільного сектору, у військові програми ... Майбутнє військового успіху тепер належатиме тим, хто розробляє, будує та використовує комбінації інформаційних технологій для забезпечення нової бойової сили”.

У широкому стратегічному та геополітичному контексті характер конфлікту змінюється, важливим стає трансформуюче технологічне середовище. Ця зміна характеру конфлікту проявляється у гібридній війні – гіпервійні, меметичній війні, кібервійні, або конфлікті наступного покоління. У кожному з них проривні технології поєднуються з існуючими технологіями та військовими можливостями для створення нових способів і засобів вступу в конфлікт. Загальними факторами, що пов'язують ці технології четвертої промислової революції, є те, що всі вони певним чином формують розумні, взаємопов'язані, розподілені та цифрові (I2D2) сили.

Майбутній науково-технічний ландшафт буде характеризуватися (і одночасно керуватися) наступним:

1) Інтелектуальність: інтегрований штучний інтелект, аналітика та можливості прийняття рішень у всьому технологічному спектрі:

- Автономія: автономні системи із штучним інтелектом, здатні до певного рівня автономного прийняття рішень. Такі автономні системи можуть бути роботизованими, заснованими на платформі або (цифровими) агентами;

- Гуманістичний інтелект: безшовна інтеграція психо-соціально-технологічних систем, що підтримують об'єднання людей та машин та синергетична поведінка;

- Аналітика знань: передові аналітичні методи (включаючи ШІ), що вивчають великі масиви даних та сучасні математичні методи, щоб надавати уявлення, знання та поради.

2) Взаємозв'язок: використання мережі (або сітки) накладання реального та віртуального доменів, включаючи датчики, організації, установи, приватних осіб, автономні агенти та процеси:

- Довірені комунікації: використання таких технологій, як технології розподіленого реєстру (наприклад, блокчейн), розподіл квантових ключів (QKD), постквантова криптографія та кібер-агенти ШІ для забезпечення надійних взаємодій та обміну інформацією;

- Синергетичні системи: розвиток змішаних (фізичних або віртуальних) складних систем, що дозволяють створювати нові екосистеми (наприклад, розумні міста).

3) Розподіленість: децентралізоване та повсюдне широкомасштабне зондування, зберігання, обчислення, прийняття рішень, дослідження та розробки:

- Edge Computing: вбудовування сховищ, обчислень та аналітики / ШІ в агенти та об'єкти, близькі до джерел інформації;

- Повсюдне зондування: вбудовування недорогих датчиків для створення великих сенсорних мереж у людських фізичних інформаційних доменах.

Додаток А – Бюджет Міністерства оборони на 2021 рік із здійснення військових досліджень і розробок для Повітряних сил США

UNCLASSIFIED

Department of the Air Force  
 FY 2021 President's Budget  
 Exhibit R-1 FY 2021 President's Budget  
 Total Obligational Authority  
 (Dollars in Thousands)

Feb 2020

Appropriation: 3600F Research, Development, Test & Eval, AF

Line No	Program Element Number	Item	Act	FY 2021 Base	FY 2021 OCO for Base Requirements	FY 2021 OCO for Direct War and Enduring Costs	FY 2021 Total OCO	FY 2021 Total (Base + OCO)	Se
1	0601102F	Defense Research Sciences	01	315,348				315,348	U
2	0601103F	University Research Initiatives	01	161,661				161,661	U
3	0601108F	High Energy Laser Research Initiatives	01	15,088				15,088	U
		<b>Basic Research</b>		<b>492,294</b>				<b>492,294</b>	
4	0602020F	Future AF Capabilities Applied Research	02	100,000				100,000	U
5	0602102F	Materials	02	140,781				140,781	U
6	0602201F	Aerospace Vehicle Technologies	02	349,228				349,228	U
7	0602202F	Human Effectiveness Applied Research	02	115,222				115,222	U
8	0602203F	Aerospace Propulsion	02						U
9	0602204F	Aerospace Sensors	02	211,301				211,301	U
10	0602212F	Defense Laboratories R&D Projects (10 U.S.C, Sec 2358)	02						U
11	0602298F	Science and Technology Management - Major Headquarters Activities	02	8,926				8,926	U
12	0602602F	Conventional Munitions	02	132,428				132,428	U
13	0602608F	Directed Energy Technology	02	128,118				128,118	U
14	0602788F	Dominant Information Sciences and Methods	02	178,668				178,668	U
15	0602890F	High Energy Laser Research	02	45,088				45,088	U
16	1206601F	Space Technology	02						U
		<b>Applied Research</b>		<b>1,409,749</b>				<b>1,409,749</b>	

UNCLASSIFIED

Page F-2A

(DOLLARS IN THOUSANDS)

Appropriation: 3600F Research, Development, Test &amp; Eval, AF

Line No	Program Element Number	Item	Act	FY 2021 Base	FY 2021 OCO for Base Requirements	FY 2021 OCO for Direct War and Enduring Costs	FY 2021 Total OCO	FY 2021 Total (Base + OCO)	See
17	0603030F	AF Foundational Development/Demos	03	103,280				103,280	U
18	0603032F	Future AF Integrated Technology Demos	03	157,619				157,619	U
19	0603033F	Next Gen Platform Dev/Demo	03	199,556				199,556	U
20	0603034F	Persistent Knowledge, Awareness, & C2 Tech	03	102,276				102,276	U
21	0603035F	Next Gen Effects Dev/Demos	03	215,817				215,817	U
22	0603112F	Advanced Materials for Weapon Systems	03						U
23	0603199F	Sustainment Science and Technology (S&T)	03						U
24	0603203F	Advanced Aerospace Sensors	03						U
25	0603211F	Aerospace Technology Dev/Demo	03						U
26	0603216F	Aerospace Propulsion and Power Technology	03						U
27	0603270F	Electronic Combat Technology	03						U
28	0603401F	Advanced Spacecraft Technology	03						U
29	0603444F	Maui Space Surveillance System (MSSS)	03						U
30	0603456F	Human Effectiveness Advanced Technology Development	03						U
31	0603601F	Conventional Weapons Technology	03						U
32	0603605F	Advanced Weapons Technology	03						U
33	0603680F	Manufacturing Technology Program	03						U

UNCLASSIFIED

Page F-3A

Appropriation: 3600F Research, Development, Test &amp; Eval, AF

Program Line Element No Number	Item	Act	FY 2021 Base	FY 2021 OCO for Base Requirements	FY 2021 OCO for Direct War and Enduring Costs	FY 2021 Total OCO	FY 2021 Total (Base + OCO)	S e c
34 0603788F	Battlespace Knowledge Development and Demonstration	03						U
35 0604445F	Wide Area Surveillance	03						U
36 0303467F	SENSR Spectrum Pipeline SRF	03						U
37 0303567F	Non-SENSR Spectrum Pipeline SRF	03						U
	Advanced Technology Development		778,548				778,548	
38 0603260F	Intelligence Advanced Development	04	4,320				4,320	U
39 0603742F	Combat Identification Technology	04	26,396				26,396	U
40 0603790F	NATO Research and Development	04	3,647				3,647	U
41 0603851F	Intercontinental Ballistic Missile - Dem/Val	04	32,959				32,959	U
42 0603859F	Pollution Prevention - Dem/Val	04						U
43 0604002F	Air Force Weather Services Research	04	869				869	U
44 0604003F	Advanced Battle Management System (ABMS)	04	302,323				302,323	U
45 0604004F	Advanced Engine Development	04	636,495				636,495	U
46 0604015F	Long Range Strike - Bomber	04	2,848,410				2,848,410	U
47 0604032F	Directed Energy Prototyping	04	20,964				20,964	U
48 0604033F	Hypersonics Prototyping	04	381,862				381,862	U
49 0604201F	FNT Resiliency, Mods, and Improvements	04						U
50 0604257F	Advanced Technology and Sensors	04	24,747				24,747	U

UNCLASSIFIED

Page F-4A

Appropriation: 3600F Research, Development, Test & Eval, AF

Line No	Program Element Number	Item	Act	FY 2021 Base	FY 2021 OCO for Base Requirements	FY 2021 OCO for Direct War and Enduring Costs	FY 2021 Total OCO	FY 2021 Total (Base + OCO)	S e c
51	0604266F	National Airborne Ops Center (NAOC) Recap	04	76,417				76,417	U
52	0604317F	Technology Transfer	04	3,011				3,011	U
53	0604327F	Hard and Deeply Buried Target Defeat System (HDBTDS) Program	04	52,921				52,921	U
54	0604414F	Cyber Resiliency of Weapon Systems-ACS	04	69,783				69,783	U
55	0604776F	Deployment & Distribution Enterprise R&D	04	25,835				25,835	U
56	0604858F	Tech Transition Program	04	219,252				219,252	U
57	0605230F	Ground Based Strategic Deterrent	04	1,524,759				1,524,759	U
58	0207100F	Light Attack Armed Reconnaissance (LAAR) Squadrons	04						U
59	0207110F	Next Generation Air Dominance	04	1,044,069				1,044,069	U
60	0207455F	Three Dimensional Long-Range Radar (3DELRR)	04	19,356				19,356	U
61	0207522F	Airbase Air Defense Systems (ABADS)	04	8,727				8,727	U
62	0208099F	Unified Platform (UP)	04	5,990				5,990	U
63	0305236F	Common Data Link Executive Agent (CDL EA)	04	39,293				39,293	U
64	0305251F	Cyberspace Operations Forces and Force Support	04						U
65	0305601F	Mission Partner Environments	04	11,430				11,430	U
66	0306250F	Cyber Operations Technology Development	04	259,823				259,823	U

UNCLASSIFIED

Page F-53

Appropriation: 3600F Research, Development, Test & Eval, AF

Line No	Program Element Number	Item	Act	FY 2021 Base	FY 2021 OCO for Base Requirements	FY 2021 OCO for Direct War and Enduring Costs	FY 2021 Total OCO	FY 2021 Total (Base + OCO)	Se
84	0604222F	Nuclear Weapons Support	05	35,033				35,033	U
85	0604270F	Electronic Warfare Development	05	2,098				2,098	U
86	0604281F	Tactical Data Networks Enterprise	05	131,909				131,909	U
87	0604287F	Physical Security Equipment	05	6,752				6,752	U
88	0604329F	Small Diameter Bomb (SDB) - EMD	05	17,280				17,280	U
89	0604429F	Airborne Electronic Attack	05						U
90	0604602F	Armament/Ordnance Development	05	23,076				23,076	U
91	0604604F	Submunitions	05	3,091				3,091	U
92	0604617F	Agile Combat Support	05	20,609				20,609	U
93	0604618F	Joint Direct Attack Munition	05	7,926				7,926	U
94	0604706F	Life Support Systems	05	23,660				23,660	U
95	0604735F	Combat Training Ranges	05	8,898				8,898	U
96	0604800F	F-35 - EMD	05	5,423				5,423	U
97	0604932F	Long Range Standoff Weapon	05	474,430				474,430	U
98	0604933F	ICBM Fuse Modernization	05	167,099				167,099	U
99	0605030F	Joint Tactical Network Center (JTNC)	05						U
100	0605056F	Open Architecture Management	05	30,547				30,547	U
101	0605221F	KC-46	05						U
102	0605223F	Advanced Pilot Training	05	248,669				248,669	U
103	0605229F	Combat Rescue Helicopter	05	63,169				63,169	U
104	0605931F	B-2 Defensive Management System	05						U

UNCLASSIFIED



Appropriation: 3600F Research, Development, Test &amp; Eval, AF

Program Line Element No Number	Item	Act	FY 2021 Base	FY 2021 OCO for Base Requirements	FY 2021 OCO for Direct War and Enduring Costs	FY 2021 Total OCO	FY 2021 Total (Base + OCO)	S e c
105 0101125F	Nuclear Weapons Modernization	05	9,683				9,683	U
106 0207171F	F-16 EPMSS	05	170,679				170,679	U
107 0207326F	Stand In Attack Weapon	05	160,438				160,438	U
108 0207701F	Full Combat Mission Training	05	9,422				9,422	U
109 0303267F	Auctioned Spectrum Relocation Fund	05						U
110 0305176F	Combat Survivor Evader Locator	05	973				973	U
111 0401221F	KC-46A Tanker Squadrons	05	106,262				106,262	U
112 0401310F	C-32 Executive Transport Recapitalization	05						U
113 0401319F	VC-25B	05	800,889				800,889	U
114 0701212F	Automated Test Systems	05	10,673				10,673	U
115 0804772F	Training Developments	05	4,479				4,479	U
116 0901299F	AF AI Systems	05	8,467				8,467	U
117 1203176F	Combat Survivor Evader Locator	05						U
118 1203269F	GPS III Follow-On (GPS IIIF)	05						U
119 1203940F	Space Situation Awareness Operations	05						U
120 1206421F	Counterspace Systems	05						U
121 1206422F	Weather System Follow-on	05						U
122 1206425F	Space Situation Awareness Systems	05						U
123 1206426F	Space Fence	05						U
124 1206431F	Advanced EHF MILSATCOM (SPACE)	05						U

UNCLASSIFIED

Page F-5A

Appropriation: 3600F Research, Development, Test & Eval, AF

Line No	Program Element Number	Item	Act	FY 2021 Base	FY 2021 OCO for Base Requirements	FY 2021 OCO for Direct War and Enduring Costs	FY 2021 Total OCO	FY 2021 Total (Base + OCO)	See
125	1206432F	Polar MILSATCOM (SPACE)	05						U
126	1206433F	Wideband Global SATCOM (SPACE)	05						U
127	1206441F	Space Based Infrared System (SBIRS) High EMD	05						U
128	1206442F	Next Generation OPIR	05						U
129	1206445F	Commercial SATCOM (COMSATCOM) Integration	05						U
130	1206553F	National Security Space Launch Program (SPACE) - EMD	05						U
System Development & Demonstration				2,615,359				2,615,359	
131	0604256F	Threat Simulator Development	06	57,725				57,725	U
132	0604759F	Major T&E Investment	06	208,680				208,680	U
133	0605101F	RAND Project Air Force	06	35,803				35,803	U
134	0605502F	Small Business Innovation Research	06						U
135	0605712F	Initial Operational Test & Evaluation	06	13,557				13,557	U
136	0605807F	Test and Evaluation Support	06	764,606				764,606	U
137	0605826F	Acq Workforce- Global Power	06						U
138	0605827F	Acq Workforce- Global Vig & Combat Sys	06						U
139	0605828F	Acq Workforce- Global Reach	06						U
140	0605829F	Acq Workforce- Cyber, Network, & Bus Sys	06						U
141	0605830F	Acq Workforce- Global Battle Mgmt	06						U

UNCLASSIFIED

Appropriation: 3600F Research, Development, Test & Eval, AF

Line No	Program Element Number	Item	Act	FY 2021 Base	FY 2021 OCO for Base Requirements	FY 2021 OCO for Direct War and Enduring Costs	FY 2021 Total OCO	FY 2021 Total (Base + OCO)	Se
142	0605831F	Acq Workforce- Capability Integration	06	1,362,038				1,362,038	U
143	0605832F	Acq Workforce- Advanced Prgm Technology	06	40,768				40,768	U
144	0605833F	Acq Workforce- Nuclear Systems	06	179,646				179,646	U
145	0605898F	Management HQ - R&D	06	5,724				5,724	U
146	0605976F	Facilities Restoration and Modernization - Test and Evaluation Support	06	70,985				70,985	U
147	0605978F	Facilities Sustainment - Test and Evaluation Support	06	29,880				29,880	U
148	0606017F	Requirements Analysis and Maturation	06	63,381				63,381	U
149	0606398F	Management HQ - TsE	06	5,785				5,785	U
150	0303255F	Command, Control, Communication, and Computers (C4) - STRATCOM	06	24,564				24,564	U
151	0308602F	ENTERPRISE INFORMATION SERVICES (EIS)	06	9,883				9,883	U
152	0702806F	Acquisition and Management Support	06	13,384				13,384	U
153	0804731F	General Skill Training	06	1,262				1,262	U
154	0909999F	Financing for Cancelled Account Adjustments	06						U
155	1001004F	International Activities	06	3,599				3,599	U
156	1206116F	Space Test and Training Range Development	06						U
157	1206392F	ACQ Workforce - Space & Missile Systems	06						U

UNCLASSIFIED

Page F-10A

## Appropriation: 3600F Research, Development, Test &amp; Eval, AF

Program Line Element No Number	Item	Act	FY 2021 Base	FY 2021 OCO for Base Requirements	FY 2021 OCO for Direct War and Enduring Costs	FY 2021 Total OCO	FY 2021 Total (Base + OCO)	S e s
158 1206398F	Space & Missile Systems Center - MHA	06						U
159 1206860F	Rocket Systems Launch Program (SPACE)	06						U
160 1206862F	Tactically Responsive Launch	06						U
161 1206864F	Space Test Program (STP)	06						U
<b>Management Support</b>			<b>2,891,280</b>				<b>2,891,280</b>	
162 0604003F	Advanced Battle Management System (ABMS)	07						U
163 0604233F	Specialized Undergraduate Flight Training	07	8,777				8,777	U
164 0604776F	Deployment & Distribution Enterprise R&D	07	499				499	U
165 0604840F	F-35 C2DC	07	785,326				785,326	U
166 0605018F	AF Integrated Personnel and Pay System (AF-IPPS)	07	27,035				27,035	U
167 0605024F	Anti-Tamper Technology Executive Agency	07	50,508				50,508	U
168 0605117F	Foreign Materiel Acquisition and Exploitation	07	71,229				71,229	U
169 0605278F	HC/MC-130 Recap RDT&E	07	24,705				24,705	U
170 0606018F	NC3 Integration	07	26,356				26,356	U
171 0606942F	Assessments and Evaluations Cyber Vulnerabilities	07						U
172 0101113F	B-52 Squadrons	07	520,023				520,023	U
173 0101122F	Air-Launched Cruise Missile (ALCM)	07	1,433				1,433	U

UNCLASSIFIED

Page F-11A

## Appropriation: 3600F Research, Development, Test &amp; Eval, AF

Line No	Program Element Number	Item	Act	FY 2021 Base	FY 2021 OCO for Base Requirements	FY 2021 OCO for Direct War and Enduring Costs	FY 2021 Total OCO	FY 2021 Total (Base + OCO)	S e c
174	0101126F	B-1B Squadrons	07	15,766				15,766	U
175	0101127F	B-2 Squadrons	07	187,399				187,399	U
176	0101213F	Minuteman Squadrons	07	116,569				116,569	U
177	0101316F	Worldwide Joint Strategic Communications	07	27,235				27,235	U
178	0101324F	Integrated Strategic Planning & Analysis Network	07	24,227				24,227	U
179	0101328F	ICBM Reentry Vehicles	07	112,753				112,753	U
181	0102110F	UH-1N Replacement Program	07	44,464				44,464	U
182	0102326F	Region/Sector Operation Control Center Modernisation Program	07	5,929				5,929	U
183	0102412F	North Warning System (NWS)	07	100				100	U
184	0205219F	MQ-9 UAV	07	162,080				162,080	U
185	0205671F	Joint Counter RCIED Electronic Warfare	07			4,080	4,080	4,080	U
186	0207131F	A-10 Squadrons	07	24,535				24,535	U
187	0207133F	F-16 Squadrons	07	223,437				223,437	U
188	0207134F	F-15E Squadrons	07	298,908				298,908	U
189	0207136F	Manned Destructive Suppression	07	14,960				14,960	U
190	0207138F	F-22A Squadrons	07	665,038				665,038	U
191	0207142F	F-35 Squadrons	07	132,229				132,229	U
192	0207146F	F-15EX	07	159,761				159,761	U
193	0207161F	Tactical AIM Missiles	07	19,417				19,417	U

UNCLASSIFIED

Page F-12A

Appropriation: 3600F Research, Development, Test &amp; Eval, AF

Line No	Program Element Number	Item	Act	FY 2021 Base	FY 2021 OCO for Base Requirements	FY 2021 OCO for Direct War and Enduring Costs	FY 2021 Total OCO	FY 2021 Total (Base + OCO)	Se
194	0207168F	Advanced Medium Range Air-to-Air Missile (AMRAAM)	07	51,799				51,799	U
195	0207227F	Combat Rescue - Pararescue	07	669				669	U
196	0207247F	AF TENCAP	07	21,644				21,644	U
197	0207249F	Precision Attack Systems Procurement	07	9,261				9,261	U
198	0207253F	Compass Call	07	15,854				15,854	U
199	0207268F	Aircraft Engine Component Improvement Program	07	95,896				95,896	U
200	0207325F	Joint Air-to-Surface Standoff Missile (JASSM)	07	70,792				70,792	U
201	0207410F	Air & Space Operations Center (AOC)	07	51,187				51,187	U
202	0207412F	Control and Reporting Center (CRC)	07	16,041				16,041	U
203	0207417F	Airborne Warning and Control System (AWACS)	07	138,303				138,303	U
204	0207418F	AFSPECWAR - TACP	07	4,223				4,223	U
206	0207431F	Combat Air Intelligence System Activities	07	16,564				16,564	U
207	0207438F	Theater Battle Management (TBM) C4I	07	7,858				7,858	U
208	0207444F	Tactical Air Control Party-Mod	07	12,906				12,906	U
209	0207448F	CSISR Tactical Data Link	07						U
210	0207452F	DCRPES	07	14,816				14,816	U
211	0207521F	Air Force Calibration Programs	07	1,970				1,970	U

UNCLASSIFIED

Page F-13A

Appropriation: 3600F Research, Development, Test &amp; Eval, AF

Line No	Program Element Number	Item	Act	FY 2021 Base	FY 2021 OCO for Base Requirements	FY 2021 OCO for Direct War and Enduring Costs	FY 2021 Total OCO	FY 2021 Total (Base + OCO)	Se
212	0207573F	National Technical Nuclear Forensics	07	396				396	U
213	0207590F	Seek Eagle	07	29,680				29,680	U
214	0207601F	USAF Modeling and Simulation	07	17,666				17,666	U
215	0207605F	Wargaming and Simulation Centers	07	6,353				6,353	U
216	0207610F	Battlefield Abn Comm Node (BACN)	07	6,827				6,827	U
217	0207697F	Distributed Training and Exercises	07	3,390				3,390	U
218	0208006F	Mission Planning Systems	07	91,768				91,768	U
219	0208007F	Tactical Deception	07	2,370				2,370	U
220	0208064F	OPERATIONAL HQ - CYBER	07	5,527				5,527	U
221	0208067F	Distributed Cyber Warfare Operations	07	68,279				68,279	U
222	0208068F	AF Defensive Cyberspace Operations	07	15,165				15,165	U
223	0208097F	Joint Cyber Command and Control (JCC2)	07	38,480				38,480	U
224	0208099F	Unified Platform (UP)	07	84,645				84,645	U
228	0208288F	Intel Data Applications	07			1,224	1,224	1,224	U
229	0301017F	Global Sensor Integrated on Network (GSIN)	07						U
230	0301025F	GeoBase	07	2,767				2,767	U
231	0301112F	Nuclear Planning and Execution System (NPES)	07	32,759				32,759	U
238	0301401F	Air Force Space and Cyber Non-Traditional ISR for Battlespace Awareness	07	2,904				2,904	U

UNCLASSIFIED

Page F-14A

Appropriation: 3600F Research, Development, Test &amp; Eval, AF

Line No	Element Number	Program Item	Act	FY 2021 Base	FY 2021 OCO for Base Requirements	FY 2021 OCO for Direct War and Enduring Costs	FY 2021 Total OCO	FY 2021 Total (Base + OCO)	See
239	0302016F	E-4B National Airborne Operations Center (NAOC)	07	3,468				3,468	U
240	0303131F	Minimum Essential Emergency Communications Network (MEECN)	07	61,887				61,887	U
241	0303133F	High Frequency Radio Systems	07						U
242	0303140F	Information Systems Security Program	07	10,351				10,351	U
243	0303142F	Global Force Management - Data Initiative	07	1,346				1,346	U
245	0304116F	Multi Domain Command and Control (MDC2)	07						U
246	0304260F	Airborne SIGINT Enterprise	07	128,110				128,110	U
247	0304310F	Commercial Economic Analysis	07	4,042				4,042	U
250	0305016F	C2 Air Operations Suite - C2 Info Services	07						U
251	0305020F	CCMD Intelligence Information Technology	07	1,649				1,649	U
252	0305022F	ISR Modernization & Automation Dvmt (IMAD)	07	19,265				19,265	U
253	0305099F	Global Air Traffic Management (GATM)	07	4,645				4,645	U
254	0305103F	Cyber Security Initiative	07	384				384	U
255	0305111F	Weather Service	07	23,640				23,640	U
256	0305114F	Air Traffic Control, Approach, and Landing System (ATCALB)	07	6,553				6,553	U
257	0305116F	Aerial Targets	07	449				449	U

UNCLASSIFIED

Page F-15A



Appropriation: 3600F Research, Development, Test &amp; Eval, AF

Line No	Program Element Number	Item	Act	FY 2021 Base	FY 2021 OCO for Base Requirements	FY 2021 OCO for Direct War and Enduring Costs	FY 2021 Total OCO	FY 2021 Total (Base + OCO)	Se
260	0305128F	Security and Investigative Activities	07	492				492	U
261	0305145F	Arms Control Implementation	07						U
262	0305146F	Defense Joint Counterintelligence Activities	07	4,890				4,890	U
264	0305179F	Integrated Broadcast Service (IBS)	07	8,864				8,864	U
265	0305202F	Dragon U-2	07	18,660				18,660	U
266	0305205F	Endurance Unmanned Aerial Vehicles	07						U
267	0305206F	Airborne Reconnaissance Systems	07	121,512				121,512	U
268	0305207F	Manned Reconnaissance Systems	07	14,711				14,711	U
269	0305208F	Distributed Common Ground/Surface Systems	07	14,152				14,152	U
270	0305220F	RQ-4 UAV	07	134,589				134,589	U
271	0305221F	Network-Centric Collaborative Targeting	07	15,049				15,049	U
272	0305238F	NATO AGS	07	36,731				36,731	U
273	0305240F	Support to DCGS Enterprise	07	33,547				33,547	U
274	0305600F	International Intelligence Technology and Architectures	07	13,635				13,635	U
275	0305861F	Rapid Cyber Acquisition	07	4,262				4,262	U
276	0305964F	Personnel Recovery Command & Ctr1 (PRC2)	07	2,207				2,207	U
277	0307577F	Intelligence Mission Data (IMD)	07	6,277				6,277	U
278	0401115F	C-130 Airlift Squadron	07	41,973				41,973	U

UNCLASSIFIED

Page F-16A

Appropriation: 3600F Research, Development, Test &amp; Eval, AF

Program Line Element No Number	Item	Act	FY 2021 Base	FY 2021 OCO for Base Requirements	FY 2021 OCO for Direct War and Enduring Costs	FY 2021 Total OCO	FY 2021 Total (Base + OCO)	S e c
279 0401119F	C-5 Airlift Squadrons (IF)	07	32,560				32,560	U
280 0401190F	C-17 Aircraft (IF)	07	9,991				9,991	U
281 0401192F	C-130J Program	07	10,674				10,674	U
282 0401194F	Large Aircraft IR Countermeasures (LAIRCM)	07	5,507				5,507	U
283 0401218F	KC-135s	07	4,591				4,591	U
284 0401219F	KC-10s	07						U
285 0401314F	Operational Support Airlift	07						U
286 0401316F	CV-22	07	18,419				18,419	U
287 0401840F	AMC Command and Control System	07						U
288 0408011F	Special Tactics / Combat Control	07	7,673				7,673	U
289 0702207F	Depot Maintenance (Non-IF)	07						U
290 0708065F	Maintenance, Repair & Overhaul System	07	24,513				24,513	U
291 0708610F	Logistics Information Technology (LOGIT)	07	35,225				35,225	U
292 0708611F	Support Systems Development	07	11,838				11,838	U
293 0804743F	Other Flight Training	07	1,332				1,332	U
294 0808716F	Other Personnel Activities	07						U
295 0901202F	Joint Personnel Recovery Agency	07	2,092				2,092	U
296 0901218F	Civilian Compensation Program	07	3,869				3,869	U
297 0901220F	Personnel Administration	07	1,584				1,584	U

UNCLASSIFIED

Page F-17A

## Appropriation: 3600F Research, Development, Test &amp; Eval, AF

Line No	Program Element Number	Item	Act	FY 2021 Base	FY 2021 OCO for Base Requirements	FY 2021 OCO for Direct War and Enduring Costs	FY 2021 Total OCO	FY 2021 Total (Base + OCO)	Se
298	0901226F	Air Force Studies and Analysis Agency	07	1,197				1,197	U
299	0901838F	Financial Management Information Systems Development	07	7,006				7,006	U
300	0901884F	Defense Enterprise Acctng and Mgt Sys (DEAMS)	07	45,638				45,638	U
301	1201017F	Global Sensor Integrated on Network (GSIN)	07	1,889				1,889	U
302	1201921F	Service Support to STRATCOM - Space Activities	07	993				993	U
303	1202140F	Service Support to SPACECOM Activities	07	8,999				8,999	U
304	1202247F	AF TENCAP	07						U
305	1203001F	Family of Advanced BLoS Terminals (FAB-T)	07						U
306	1203110F	Satellite Control Network (SPACE)	07						U
308	1203165F	NAVSTAR Global Positioning System (Space and Control Segments)	07						U
309	1203173F	Space and Missile Test and Evaluation Center	07						U
310	1203174F	Space Innovation, Integration and Rapid Technology Development	07						U
311	1203179F	Integrated Broadcast Service (IBS)	07						U
312	1203182F	Spacelift Range System (SPACE)	07						U
313	1203265F	GPS III Space Segment	07						U
314	1203400F	Space Superiority Intelligence	07	16,810				16,810	U

UNCLASSIFIED

Page F-16A

## Appropriation: 3600F Research, Development, Test &amp; Eval, AF

Line No	Element Number	Program Item	Act	FY 2021 Base	FY 2021 OCO for Base Requirements	FY 2021 OCO for Direct War and Enduring Costs	FY 2021 Total OCO	FY 2021 Total (Base + OCO)	Se
315	1203614F	JSpOC Mission System	07						U
316	1203620F	National Space Defense Center	07	2,687				2,687	U
317	1203873F	Ballistic Missile Defense Radars	07						U
318	1203906F	NCMC - TW/AA System	07	6,990				6,990	U
319	1203913F	NUDET Detection System (SPACE)	07						U
320	1203940F	Space Situation Awareness Operations	07						U
321	1206423F	Global Positioning System III - Operational Control Segment	07						U
322	1206770F	Enterprise Ground Services	07						U
9999	9999999999	Classified Programs		15,777,856				15,777,856	U
		Operational Systems Development		21,466,680		5,304	5,304	21,471,984	
		<b>Total Research, Development, Test &amp; Eval, AF</b>		<b>37,391,826</b>		<b>5,304</b>	<b>5,304</b>	<b>37,397,130</b>	

Джерело: RDT&E PROGRAMS (R-1). Department of Defense Budget. Fiscal Year 2021 [Електронний ресурс]. - Office of the Under Secretary of Defense (Comptroller). - Feb 2020. - 242 p. - Режим доступу: [https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2021/fy2021\\_r1.pdf](https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2021/fy2021_r1.pdf)

## СПИСОК ПОСИЛАНЬ

- 
- 1 Emerging military and security technologies. – STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE. [Электронный ресурс]. – Режим доступа: <https://www.sipri.org/research/armament-and-disarmament/emerging-military-and-security-technologies>
  - 2 INTEGRATED REVIEW: CALL FOR EVIDENCE [Электронный ресурс]. – Режим доступа: <https://www.gov.uk/government/publications/integrated-review-call-for-evidence>
  - 3 Global warming of 1.5°C [Электронный ресурс]. – Режим доступа: [https://report.ipcc.ch/sr15/pdf/sr15\\_spm\\_final.pdf](https://report.ipcc.ch/sr15/pdf/sr15_spm_final.pdf)
  - 4 UN Report: Nature’s Dangerous Decline ‘Unprecedented’; Species Extinction Rates ‘Accelerating’ [Электронный ресурс]. – Режим доступа: <https://www.un.org/sustainabledevelopment/blog/2019/05/nature-decline-unprecedented-report/>
  - 5 The 100 largest companies in the world by market capitalization in 2020 [Электронный ресурс]. – Режим доступа: <https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-capitalization/>
  - 6 Growing consumption [Электронный ресурс]. – Режим доступа: [https://ec.europa.eu/knowledge4policy/growing-consumerism\\_en](https://ec.europa.eu/knowledge4policy/growing-consumerism_en)
  - 7 Therése Pettersson Organized violence, 1989–2019 [Электронный ресурс]/ Therése Pettersson, Magnus Öberg // Journal of Peace Research, 2020. - vol. 57, № 4. - pp. 597-613. - Режим доступа: <https://journals.sagepub.com/doi/pdf/10.1177/0022343320934986>
  - 8 States of Fragility 2018 [Электронный ресурс]. – Режим доступа: [https://www.oecd.org/dac/conflict-fragility-resilience/docs/OECD%20Highlights%20documents\\_web.pdf](https://www.oecd.org/dac/conflict-fragility-resilience/docs/OECD%20Highlights%20documents_web.pdf)
  - 9 Bidwell, C. & MacDonald, B. Emerging Disruptive Technologies and Their Potential Threat to Strategic Stability and National Security. Tech. Rep., Federation of American Scientists (2018). [Электронный ресурс]. – Режим доступа: <https://fas.org/wp-content/uploads/media/FAS-Emerging-Technologies-Report.pdf>
  - 10 Crow, L. Demis Hassabis on AI’s potential (2020). URL <https://theworldin.economist.com/edition/2020/article/17385/demis-hassabis-ais-potential>
  - 11 Cybersecurity [Электронный ресурс]. – Режим доступа: <https://intelligence.weforum.org/topics/a1Gb00000015LbsEAE?tab=publications>
  - 12 Federated Interoperability of Military C2 and IoT Systems [Электронный ресурс]. – Режим доступа: [https://www.sto.nato.int/Pages/technical-team.aspx?k=\(\\*\)&s=Search%20IST%20Activities&View=%7b2C52FF39-CB1C-4A13-8129-6976E923EDEC%7d&FilterField1=ACTIVITY%5FPANEL&FilterValue1=IST](https://www.sto.nato.int/Pages/technical-team.aspx?k=(*)&s=Search%20IST%20Activities&View=%7b2C52FF39-CB1C-4A13-8129-6976E923EDEC%7d&FilterField1=ACTIVITY%5FPANEL&FilterValue1=IST)
  - 13 WIPO Technology Trends 2019 – Artificial Intelligence [Электронный ресурс]. – Режим доступа: <https://www.wipo.int/publications/en/details.jsp?id=4386>
  - 14 AI 100: The Artificial Intelligence Startups Redefining Industries, CB Insights, March 3, 2020. - [Электронный ресурс]. – Режим доступа: <https://www.cbinsights.com/research/artificial-intelligence-top-startups/>.

---

15 Указ Президента Российской Федерации от 10.10.2019 № 490 “О развитии искусственного интеллекта в Российской Федерации“. – 2019. - [Электронный ресурс]. – Режим доступа: <http://publication.pravo.gov.ru/Document/View/0001201910110003> .

16 Samuel Bendett, “Here’s How the Russian Military Is Organizing to Develop AI,” *Defense One*, July 2018. - [Электронный ресурс]. – Режим доступа: <https://www.defenseone.com/ideas/2018/07/russian-militarys-ai-development-roadmap/149900/>

17 Фонд перспективных исследований [Электронный ресурс]. – Режим доступа: <https://fpi.gov.ru/>

18 Alina Polyakova Weapons of the Weak: Russia and AI-driven Asymmetric Warfare // Brookings Institution, November 15, 2018. - <https://www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/>

19 Franklin, J., Carmody, C., Keller, K., Levitt, T. & Buteau, V. Expert system technology for the military: selected samples. Proceedings of the IEEE 76, 1327–1366 (1988). URL <http://ieeexplore.ieee.org/document/16329/>

20 Intel. Neuromorphic Computing - Next Generation of AI (2019). URL <https://www.intel.com/content/www/uk/en/research/neuromorphic-computing.html>

21 Bufithis, G. Oh, crap! Even MORE stuff to worry about: malevolent machine learning can derail AI (thank you, Enron data set!) / Gregory Bufithis. – 2019. - [Электронный ресурс]. – Режим доступа: <http://www.gregorybufithis.com/2019/03/26/oh-crap-even-more-stuff-to-worry-about-malevolent-machine-learning-could-derail-ai/>

22 Artificial Intelligence Research Associate (AIRA) [Электронный ресурс]. – Режим доступа: <https://www.darpa.mil/program/artificial-intelligence-research-associate>

23 DARPA. Defense Advanced Research Projects Agency. Budget Estimates FY 2020. RDT&E Program. Tech. Rep. - DARPA, 2019. - [Электронный ресурс]. – Режим доступа: [https://www.darpa.mil/attachments/DARPA\\_FY20\\_Presidents\\_Budget\\_Request.pdf](https://www.darpa.mil/attachments/DARPA_FY20_Presidents_Budget_Request.pdf)

24 Глобальная индустрия ИИ, 2020. - <https://www.reportlinker.com/p05478480/Global-Artificial-Intelligence-AI-Industry.html>

25 Market share held by the leading Windows anti-malware application vendors worldwide, as of April 2020 [Электронный ресурс]. – Режим доступа: <https://www.statista.com/statistics/271048/market-share-held-by-antivirus-vendors-for-windows-systems/>

26 Fiscal Year (FY) 2021 Budget Estimates. - Department of Defence Information Technology and cyberspace Activities Budget Overview, 2020. - [Электронный ресурс]. – Режим доступа: [https://www.cape.osd.mil/content/SNAPIT/files/FY21/FY21%20DoD%20IT-CA%20Budget%20Overview\\_Approved.pdf](https://www.cape.osd.mil/content/SNAPIT/files/FY21/FY21%20DoD%20IT-CA%20Budget%20Overview_Approved.pdf)

27 White House issues new cybersecurity policy for space systems [Электронный ресурс]. – Режим доступа: [https://www.c4isrnet.com/battlefield-tech/space/2020/09/04/white-house-issues-new-cybersecurity-policy-for-space-systems/?utm\\_source=Sailthru&utm\\_medium=email&utm\\_campaign=C4ISRNET%20Daily%2009.8&utm\\_content=Final&utm\\_term=Editorial%20-%20Daily%20Brief](https://www.c4isrnet.com/battlefield-tech/space/2020/09/04/white-house-issues-new-cybersecurity-policy-for-space-systems/?utm_source=Sailthru&utm_medium=email&utm_campaign=C4ISRNET%20Daily%2009.8&utm_content=Final&utm_term=Editorial%20-%20Daily%20Brief)

---

28 THE TAXONOMY OF THE ECSO. CYBERSECURITY MARKET RADAR. – ECSO, 2020. – 12 pp. - [Електронний ресурс]. – Режим доступу: [https://www.ecso.org.eu/documents/uploads/ecso-cybersecurity-market-radar-brochure\\_20190911\\_10\\_14\\_26.pdf](https://www.ecso.org.eu/documents/uploads/ecso-cybersecurity-market-radar-brochure_20190911_10_14_26.pdf)

29 Securing cyberspace: Concrete results through EU research and innovation [Електронний ресурс]. – Режим доступу: <https://cordis.europa.eu/article/id/400141-securing-cyberspace-delivering-concrete-results-through-eu-research-and-innovation>

30 Speech by Executive Vice-President Margrethe Vestager on the Digital Package [Електронний ресурс]. – Режим доступу: [https://ec.europa.eu/commission/presscorner/detail/en/SPEECH\\_20\\_1704](https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1704)

31 Cyber Security [Електронний ресурс]. – Режим доступу: <https://www.marketresearch.com/Global-Industry-Analysts-v1039/Cyber-Security-13496962/>

32 Zacharias G. Autonomous horizons: the way forward / G. Zacharias. - Alabama: Air University Press ; Curtis E. LeMay Center for Doctrine Development and Education, Maxwell Air Force Base, 2019.

33 Williams A. P. Autonomous Systems - Issues for Defence Policy Makers / Williams A. P. & Scharre, P. D. (eds.). - Norfolk, VA: NATO Allied Command Transformation, 2015. - [Електронний ресурс]. – Режим доступу: [http://www.act.nato.int/images/stories/media/capdev/capdev\\_02.pdf](http://www.act.nato.int/images/stories/media/capdev/capdev_02.pdf).

34 Army A. Robotic & Autonomous Systems Strategy. - Tech. Rep. - Commonwealth of Australia, Canberra, Australia, 2018. [Електронний ресурс]. – Режим доступу: <https://www.army.gov.au/our-future/australian-army-research-centre-aarc/australian-army-research-centre-publications/robotic> .

35 Rane S. Building a cyber-physical immune system [Електронний ресурс]. – Режим доступу: <https://www.computerweekly.com/opinion/Building-a-cyber-physical-immune-system>

36 Military Robots Market by Platform (Land, Marine, Airborne), Application (ISR, Search and Rescue, Combat Support, Transportation, EOD, Mine Clearance, Firefighting), Mode of Operation (Human Operated, Autonomous), and Region - Global Forecast to 2022 [Електронний ресурс]. – Режим доступу: <https://www.marketsandmarkets.com/Market-Reports/military-robots-market-245516013.html>

37 Кваша Т.К. Світові наукові та технологічні тренди у сфері забезпечення національної безпеки: наукова доповідь / Т.К. Кваша. - Київ: УкрІНТЕІ, 2019. – 99 с. - ISBN 978-966-479-109-7. DOI: 10.35668/978-966-479-109-7

<sup>38</sup> *Science & Technology Trends 2020-2040*. Exploring the S&T Edge. NATO Science & Technology Organization, 160.

39 DEFENSE SPACE STRATEGY. SUMMARY [Електронний ресурс]. – Режим доступу: [https://media.defense.gov/2020/Jun/17/2002317391/-1/-1/1/2020\\_DEFENSE\\_SPACE\\_STRATEGY\\_SUMMARY.PDF](https://media.defense.gov/2020/Jun/17/2002317391/-1/-1/1/2020_DEFENSE_SPACE_STRATEGY_SUMMARY.PDF)

40 SIPRI Yearbook 2020 [Електронний ресурс]. – Режим доступу: [https://www.sipri.org/sites/default/files/2020-06/yb20\\_summary\\_en\\_v2.pdf](https://www.sipri.org/sites/default/files/2020-06/yb20_summary_en_v2.pdf)

41 Erin Duffin Nuclear weapons - Statistics & Facts [Електронний ресурс]. – Режим доступу: <https://www.statista.com/topics/4269/nuclear-weapons/>

---

42 Американский тактический гиперзвуковой планер получит дальность до 1600 километров [Электронный ресурс]. – Режим доступа: <https://nplus1.ru/news/2020/10/24/opfires>

43 National Defense strategy of The United States of America. URL: <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>

44 Implementing the National Defense Strategy: A Year of Successes [Электронный ресурс]. – Режим доступа: <https://media.defense.gov/2020/Jul/17/2002459291/-1/-1/1/NDS-FIRST-YEAR-ACCOMPLISHMENTS-FINAL.pdf>

45 Army Modernization Strategy [Электронный ресурс]. – Режим доступа: [https://www.army.mil/e2/downloads/rv7/2019\\_army\\_modernization\\_strategy\\_final.pdf](https://www.army.mil/e2/downloads/rv7/2019_army_modernization_strategy_final.pdf)

46 FY 2021 President's Budget Highlights, US Army Budget Overview. – US Assistant Secretary of the Army (Financial Management and Comptroller), 2020 – pp. 38. - <https://www.hsdl.org/?view&did=834751>

47 Применение элементов искусственного интеллекта в беспилотных летательных аппаратах ВС США [Электронный ресурс]. – Режим доступа: [http://pentagonus.ru/publ/primenenie\\_elementov\\_iskusstvennogo\\_intellekta\\_v\\_bespilotnykh\\_le\\_tatelnykh\\_apparatakh\\_vs\\_ssha\\_2020/16-1-0-2927](http://pentagonus.ru/publ/primenenie_elementov_iskusstvennogo_intellekta_v_bespilotnykh_le_tatelnykh_apparatakh_vs_ssha_2020/16-1-0-2927)

48 Америка ушла в космос. Новая стратегия должна обеспечить США глобальное превосходство [Электронный ресурс]. – Режим доступа: [https://www.ng.ru/armies/2020-06-22/8\\_7891\\_space.html](https://www.ng.ru/armies/2020-06-22/8_7891_space.html)

49 RDT&E PROGRAMS (R-1). Department of Defense Budget. Fiscal Year 2021 [Электронный ресурс]. - Office of the Under Secretary of Defense (Comptroller). - Feb 2020. – 242 p. - Режим доступа: [https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2021/fy2021\\_r1.pdf](https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2021/fy2021_r1.pdf)

50 Air Force. Justification Book Volume 1 of 1. Research, Development, Test & Evaluation, Space Force. - Department of Defense. Fiscal Year (FY) 2021. Budget Estimates. – 2020. – 368 pp.

51 Defense Advanced Research Projects Agency. Program Information. Our Research [Электронный ресурс]. – Режим доступа: <https://www.darpa.mil/program/our-research/more>



---

*Наукове видання*

**Писаренко Тетяна Василівна**

**Кваша Тетяна Костянтинівна**

**Глобальні технологічні тренди  
у сфері озброєння та військової техніки**

Матеріали друкуються в авторській редакції

Формат: PDF

Об'єм даних 2,43 Мб.

Інтернет-адреса видання: [www.uitei.kiev.ua/sites/default/files/Ozbron\\_tech.pdf](http://www.uitei.kiev.ua/sites/default/files/Ozbron_tech.pdf)

Верстка та оригінал-макет: Т. Кваша

Редакція: ДНУ «Український інститут науково-технічної  
експертизи та інформації» (УкрІНТЕІ)  
03150, м. Київ, вул. Антоновича, 180  
Тел. (044) 521-00-10, e-mail: [uitei@uitei.kiev.ua](mailto:uitei@uitei.kiev.ua)  
Свідоцтво суб'єкта видавничої справи  
ДК № 5332 від 12.04.2017 р.