發改委：鞏固拓展經濟回升向好勢頭

治理企業無序競爭 推進價格法修訂

【大公報訊】記者任芳頡北京報道：國家發改委1日召開新聞發布會，解讀當前經濟形勢和經濟工作。發改委國民經濟綜合司司長周陳介紹，上半年中國經濟在頂住外部壓力、消化累積風險的情況下，穩中有進、好於預期。上半年國內生產總值（GDP）同比增長5.3%，比去年同期和全年均提高0.3個百分點。「近期多家國際機構上調今年全年中國經濟增速預測，國際貨幣基金組織前幾天大幅上調了預測，表明對中國經濟發展前景充滿信心。」

宏觀政策將持續發力適時加力

為鞏固拓展經濟回升向好勢頭，發改委明確，我國宏觀政策將持續發力、適時加力。周陳表示，發改委將努力完成全年經濟社會發展預期目標和「十四五」規劃各項任務，為「十五五」良好開局打下基礎。一方面，持續發力、適時加力實施好已部署的各項政策舉措，堅定不移實施擴大內需戰略，堅定不移推動高水平科技自立自強，深化改革開放，加力建設全國統一大市場，特別是繼續推動穩就業穩經濟若干舉措陸續出台實施，保持政策連續性、穩定性，增強靈活性、預見性，將外部壓力轉化為內生動力，穩住經濟大盤。另一方面，將常態化開展政策預研儲備，不斷完善穩就業、擴內需政策「工具箱」，根據實際需要及時推出。

發改委政策研究室主任蔣毅介紹，今年第三批690億元支持消費品以舊換新的超長期特別國債資金已下達完畢，將於10月份按計劃下達第四批690億元（人民幣，下同）資金，屆時將完成全年3000億元的下達計劃。此外，今年「兩重」建設項目清單8000億元已全部下達完畢，中央預算內投資7350億元已基本下達完畢。

發改委表示，將進一步規範政府行為尺度，制定《妨礙統一市場和公平競爭行為防範事項清單》。依法依規治理企業無序競爭，推進重點行業產能治理，加快推進價格法修訂，將重點治理為排擠競爭對手或獨佔市場，低於成本價傾銷的行為。規範招標投標，規範地方招商引資行為。周陳表示，鼓勵創新與適度競爭，遏制盲目跟風及「一哄而上、一哄而散」現象，破除「內捲式競爭」。發改委指出，在創新方面，將深入實施「人工智能＋」行動，大力推進人工智能規模化商業化應用，着力優化人工智能創新生態，加大政策支持力度。

中國經濟穩中有進好於預期

經濟增長 上半年我國GDP為660536億元（人民幣，下同），同比增長5.3%，增速比去年同期和全年均提升0.3個百分點。

就業 上半年全國城鎮調查失業率平均值為5.2%，比一季度下降0.1個百分點。其中，6月份全國城鎮調查失業率為5%。

國際收支 上半年貨物進出口總額創同期新高；6月末，我國外匯儲備規模為33174億美元，連續19個月穩定在3.2萬億美元以上，並連續6個月保持增長。

消費 上半年最終消費支出對經濟增長的貢獻率為52%。上半年社會消費品零售總額為24.55萬億元，同比增長5%。

大公報記者任芳頡整理

人民日報：英偉達，讓我怎麼相信你？

人民日報1日發表題為《英偉達，讓我怎麼相信你？》的評論。文章指出，英偉達算力芯片H20被曝出存在嚴重安全問題，公司最近被國家網信辦約談。事後，英偉達出來回應：「網絡安全對我們至關重要。英偉達的芯片不存在『後門』，並不會讓任何人有遠程訪問或控制這些芯片的途徑。」

文章指出，回應歸回應，企業唯有按照約談要求，拿出令人信服的安全證明，才能消除中國用戶的後顧之憂，重新贏得市場信任。發展數字經濟、建設數字中國，必須維護好網絡空間安全，絕不能讓「帶病」的芯片上崗。

美情報機構借盟友做「跳板」網攻中國竊國防軍工機密

▲內地舉行大型網絡安全比賽，加速發掘專門人才，應對新型風險挑戰。

焦點追蹤

「這是美國政府對中國實施惡意網絡攻擊的最新證據，再次表明美國是中國面臨的頭號網絡威脅，也暴露了美國在網絡安全上賊喊捉賊的虛偽面目。中國將繼續採取必要措施維護自身的網絡安全。」外交部發言人郭嘉昆1日在答問時說。

據中國網絡空間安全協會（下稱協會）1日消息，美國情報機構近年來將網絡攻擊竊密的重點目標瞄準中國高科技軍工類的高校、科研院所及企業，試圖竊取中國軍事領域相關的科研數據或設計、研發、製造等環節的核心生產數據等敏感信息，嚴重威脅中國國防軍工領域的科研生產安全甚至國家安全。協會公布兩起典型案例均顯示，美國政府通過德國、韓國、新加坡、荷蘭等盟友作為「跳板」對華實施網攻。

掃一掃有片睇

大公報記者 蘇雨潤

協會引用中國國家互聯網應急中心（CNCERT）的監測結果指出，美國情報機構將網絡攻擊竊密的重點目標瞄準中國高科技軍工類的高校、科研院所及企業，目標更有針對性、手法更加隱蔽。

第一個案例是2022年7月至2023年7月，美情報機構利用微軟Exchange郵件系統零日漏洞，對中國一家大型重要軍工企業的郵件服務器攻擊並控制將近1年。經調查，攻擊者控制該企業域控服務器，以域控服務器為跳板，控制內網中50餘台重要設備，並在企業的某對外工作專用服務器中植入建立websocket+SSH隧道的攻擊竊密武器，意圖實現持久控制。同時，攻擊者在該企業網絡中構建多條隱蔽通道進行數據竊取。

第二個案例是2024年7月至11月，美情報機構對中國某通信和衛星互聯網領域的軍工企業實施網絡攻擊。經調查，攻擊者先是通過位於羅馬尼亞（72.5.*.*）、荷蘭（167.172.*.*）等多個國家的跳板IP，利用未授權訪問漏洞及SQL注入漏洞攻擊該企業電子文件系統，向該企業電子文件服務器植入內存後門程序並進一步上傳木馬，在木馬攜帶的惡意載荷解碼後，將惡意載荷添加至Tomcat（美國Apache基金會支持的開源代碼Web應用服務器項目）服務的過濾器，通過檢測流量中的惡意請求，實現與後門的通信。隨後，攻擊者又利用該企業系統軟件升級服務，向該企業內網定向投遞竊密木馬，入侵控制了300餘台設備，並搜索「軍專網」、「核心網」等關鍵詞定向竊取被控主機上的敏感數據。

去年中國重要單位遭網攻逾600次

協會披露，僅2024年境外國家級APT（高級持續性威脅）組織對中國重要單位的網絡攻擊事件就超過600起，其中國防軍工領域是受攻擊的首要目標。尤其是以美國情報機構為背景的黑客組織依託成建制的網攻團隊、龐大的支撐工程體系與制式化的攻擊裝備庫、強大的漏洞分析挖掘能力，對中國關鍵信息基礎設施、重要信息系統、關鍵人員等進行攻擊滲透，嚴重威脅中國國家網絡安全。亞洲視覺科技研發總監陳經向《大公報》表示，美國對全球多國實施無差別網攻，還通過媒體和官方文件潑污水，蓄意將中企塑造成「網絡威脅者」，其真實目的無非是為自身的技術遏制、市場封鎖及預算擴張尋找藉口。中國必須以強大技術實力為支撐，秉持「安全前置」戰略思維，在網絡基礎設施中全面推廣安全防護機制。

專家：強化信息基建 保障AI安全應用

陳經認為，要推動《關鍵信息基礎設施安全條例》的細化落地，明確AI訓練平台、大模型服務商的安全責任邊界，建立涵蓋數據出境、模型調用、API接口的全流程安全評估標準。具體而言，可研建「安全認證」制度，由國家網信部門授權第三方機構對科研院所、科創企業開展攻防測試與安全評級，以此作為相關機構開展活動的安全性參考依據。並且，以「一帶一路」倡議為紐帶，與全球多國共建跨境數據安全通道，推廣中國安全技術標準與設備，逐步降低對美歐不可靠網絡通信設備的依賴。

兩大漏洞

利用微軟Exchange郵件系統零日漏洞

攻擊時間	2022年7月至2023年7月
攻擊者	美國情報機構
目標	內地一家大型重要軍工企業的郵件伺服器
攻擊手段	• 利用微軟Exchange郵件系統零日漏洞 • 控制域控伺服器，以域控伺服器為跳板，控制內網50餘台重要設備 • 在某對外工作專用伺服器中植入建立websocket+SSH隧道的攻擊竊密武器，實現持久控制 • 構建多條隱蔽通道進行數據竊取
攻擊路徑	使用跳板IP：德國(159.69..)、芬蘭(95.216..)、韓國(158.247..)、新加坡(139.180..)
次數	發起40餘次網攻
竊取內容	包括企業高層在內11人的郵件，涉及軍工類產品的設計方案、系統核心參數。

利用電子文件系統漏洞

攻擊時間	2024年7月至11月
攻擊者	美國情報機構
目標	內地某通信和衛星互聯網領域的軍工企業
攻擊手段	• 利用未授權訪問漏洞及SQL注入漏洞攻擊電子文件系統。 • 向電子文件伺服器植入內存後門程式並上傳木馬。 • 木馬惡意載荷解碼後，添加至Tomcat服務的過濾器，通過檢測流量中的惡意請求實現與後門通信。 • 利用系統軟件升級服務定向投遞竊密木馬，入侵控制內網300餘台設備。
攻擊路徑	使用跳板IP：羅馬尼亞(72.5..)、荷蘭(167.172..)
竊取內容	搜索「軍專網」、「核心網」等關鍵詞，定向竊取被控主機敏感數據。

國家互聯網應急中心 曝光美網攻手法

▲對於美國頻繁對華實施網攻竊密，專家建議推動立法，明確AI訓練平台、大模型服務商的安全責任邊界，堵塞潛在漏洞。圖為去年在廣州舉行的網絡安全博覽會，華為展示尖端網絡安全產品。

三招隱匿

- **聲東擊西**：通過混淆逃避安全軟件監測
- **加密偽裝**：以加密方式抹去惡意通信特徵
- **多層滲透**：多層流量轉發攻擊重要設備

資料來源：「中國網絡空間安全協會」微信公眾號

▼今年2月3日，《大公報》專題報道揭露，國產大模型DeepSeek遭受大規模「殭屍網攻」，幕後黑手來自美國IP。

DeepSeek曾遭「殭屍網攻」美國IP幕後黑手

特稿

今年年初，國產AI大模型DeepSeek憑藉其在數學、代碼、自然語言推理等任務上的優質性能，在多個平台上線後廣受歡迎。然而，其線上服務卻在1月底突然遭遇大規模網絡攻擊，多次出現服務中斷現象。

DeepSeek從1月初開始便持續遭受定期的分布式拒絕服務（DDoS）攻擊，除動用反射放大技術，還發起來自美國IP地址的HTTP代理攻擊及暴力破解嘗試。奇安信XLab實驗室通過持續近1個月監測發現：攻擊模式從最初的「易被清洗放大攻擊」，升級至1月28日的HTTP代理攻擊（應用層攻擊，防禦難度提升），到大年初二（1月30日）凌晨，亦即是DeepSeek登頂下載榜未幾，攻擊烈度大增，指令暴增上百倍，至少有2個殭屍網絡（botnet）參與攻擊。

在這場被網友們稱為數字時代「上甘嶺」的戰役中，360、奇安信、華為等多家中企與DeepSeek聯手抵禦攻擊，愈戰愈勇，黑客節節敗退。