矽生命線：

俄羅斯戰爭機器中的西方電子產品

JAMES BYRNE, GARY SOMERVILLE, JOE BYRNE,
JACK WATLING, NICK REYNOLDS 及 JANE BAKER

2022年8月

聲明：

本文件由RUSI編寫，僅供參考用途（「許可用途」）。儘管RUSI已採取一切合理謹慎措施以確保本報告所包含資料（「資料」）準確，但該等資料主要來自烏克蘭實地調查及公開來源，RUSI不就該等資料作出任何形式的聲明或保證。

不得超出「許可用途」以任何其它目的使用、複製或依賴「資料」。對「資料」內容的任何依賴，風險自負。如意圖將「資料」用於任何其它目的（包括但不限於啟動法律程序、採取措施或拒絕採取措施或以其它方式與任何指定的個人或實體進行交涉），則必須首先開展自己的獨立研究並據此來核實「資料」。

在法律允許的最大限度內，RUSI不對讀者本人或任何第三方因複制、依賴或使用任何「資料」而引起的損失或損害，或與之有關的任何性質的可預見或不可預見的任何損失或損害（包括但不限於誹謗）承擔責任。報告提及RUSI時包括其董事和員工。

在本報告中，作者對俄文和中文記錄的公司、實體和個人名稱進行了處理。在某些情況下，不得不將公司、实体和个人的名称翻譯或音譯。作者已盡一切努力確保翻譯/音譯的準確性，不對此方面的任何無意錯誤承擔責任。

作者還處理了帶有序列號的大型微電子元件數據集，通過驗證它們的真實性並使用開源資訊解析出其相應的製造商。但其中一小部分在製造商網頁或第三方賣家網頁上無法被找到，可能是因為這些序列號對應的產品現已停產。此外，有些零部件的可識別信息不充分，因此無法對其作出肯定的鑑定。

本報告對個人、公司和政府的鑑別

本報告的目的是解釋和展示俄羅斯軍隊如何依賴西方技術。為了實現這一目的，報告找出了一些被認為參與了設計和製造由俄羅斯軍方獲得併用於其軍事武器中的零部件的個人、公司、政府。為免生疑問，除非在報告中明確指出，否則RUSI不指控這些個人/公司/政府的任何不法行為，也不指出或斷言這些個人/公司/政府參與了任何逃避制裁的相關活動，或違反了限製或禁止此類行動的任何國際（或其本國）法律或法規，直接或間接向俄羅斯軍隊和/或俄羅斯軍事客戶供貨。

方法

在本報告中，RUSI的開源情報與分析（OSIA）和軍事科學部門用到了大量的零部件和微電子數據集，它們均來源於拆卸自2022年2月以來在烏克蘭尋獲或消耗的俄羅斯武器。這些技術評估被彙編成數據庫，經標準化和分類處理，以作進一步分析。

RUSI在實地工作期間對武器系統和平台的大量樣本進行了實物檢查，並與製造商發布的產品描述和序列號進行了比較，證實了這些數據的真實性和準確性。但應指出，全球充斥着銷售假冒零部件和微電子的灰市和黑市，要保證證據無誤絕非易事。鑑於報告中所評估的證據，以及蘇聯和俄羅斯以世界領先技術和微電子公司為目標建立軍事採購網絡的長期歷史，研究小組的工作基於這些零部件中大多數為真品的假設。由俄羅斯政府內部進行的、作者們所見的評估都強調了俄羅斯對一些外國製造商的嚴重依賴這一事實，這讓作者們對俄羅斯武器中識別出的零部件的真實性更有信心。未來還可對這些平台中發現的許多零部件作進一步檢查，特別是採用X射線分析，以驗證其真實性。然而，烏克蘭持續的衝突為進一步研

究帶來了挑戰。

因此，作者將這些數據與一系列其他來源的數據結合，如運輸級別的貿易數據、進出口申報和俄羅斯的公司記錄，同時也將涉及到的武器放在戰術、作戰和戰略背景下，以期更好地了解俄羅斯的國家採購網絡。

致謝

RUSI謹此感謝為本報告提供幫助的幾位人士和合作夥伴，包括Peter Roberts教授、Markus Schiller博士、Daniel Salisbury博士和Sean Corbett CB MBE。並特此感謝Altana Technologies，他們的Altana Atlas數據平台幫助了我們了解半導體和微電子產品是如何通過國際貿易系統進入俄羅斯軍方最終用戶的。

IN PARTNERSHIP WITH Altana

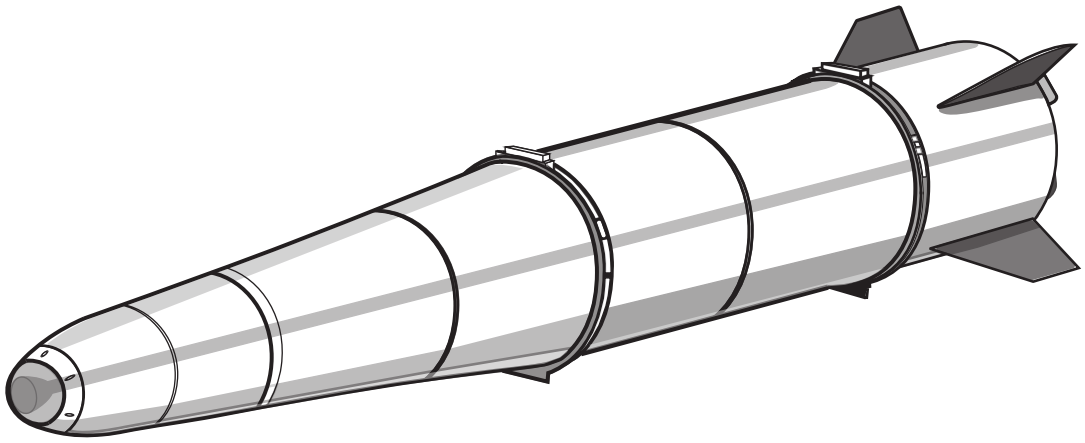
版權

©皇家國防安全聯合軍種研究所，2022年

本文獲得知識共享署名—非商業性使用—禁止演繹4.0協議國際版許可。有關許可的更多詳情，請訪問<http://creativecommons.org/licenses/by-nc-nd/4.0/>。

更正通知，2022年8月8日

請注意，本報告的更早版本錯誤地將總部位於美國的公司Gumstix稱為德國公司。已對此進行了更正，所有相關數據均已被相應更新。作者及RUSI



伊斯坎德爾導彈外形　來源：RUSI.

内容

概要 5

引言 7

第 1 部分：武器系統及西方零部件 11

全球採購 13

堵住供應渠道：制裁與出口管制 15

美國頭號通緝犯 17

大盜亞德諾 22

德州一切更美好 24

東京罪惡 25

各盡所能，各取所需 27

鎖定瑞士 28

打通荷蘭 28

攻克倫敦 28

滲透柏林 29

第 2 部分：俄羅斯導彈的剖析 33

伊斯坎德爾9M727 34

Zarya雷達處理計算機 35

Baget計算機 38

導航系統 41

多種產品 43

Kh-101巡航導彈 45

第 3 部分：漏洞：零部件流入俄羅斯 47

一條全球性供應鏈：俄羅斯半導體進口 47

深探戰場 51

追踪受制裁實體 52

香港芯片店 53

結論 57

作者介紹 58

概要

俄羅斯於2022年2月24日入侵烏克蘭，然而戰爭並未如期望的那樣進展。原先被認為會是一次對烏克蘭各城市外科手術式的佔領行動，現在卻已成為一場曠日持久的消耗戰，這場戰爭正在迅速削弱俄羅斯軍隊的實力。本報告對俄羅斯27套最現代化的軍事系統的零部件及其功能進行了研究，這些系統包括巡航導彈、通信系統和電子戰綜合系統。最後得出的結論認為，如果實施恰當的政策，就可能永久性地削弱俄羅斯的軍事能力。

報告基於對在烏克蘭尋獲或向烏克蘭發射的俄羅斯軍事裝備的技術檢查結果，闡述了俄羅斯耗資數十億美元、歷時數十年的軍事現代化計劃是如何依賴美國、日本、台灣、韓國、瑞士、荷蘭、英國、法國和德國製造的微電子技術的支持的。俄羅斯公司若要在軍事裝備中使用外國零部件，必須向其國防部證明 國內沒有替代品。

RUSI在這27個武器系統中至少發現了450種外國製造的各種獨特零部件，其中大部分由那些在為美國軍方設計和製造複雜微電子技術方面有着久負盛名的美國製造商製造。這其中至少有80種不同零部件是受到美國出口管制的，這表明俄羅斯的軍工複合體在近幾十年來成功地規避了這些管制。本報告詳細例舉了從蘇聯時代到2022年俄羅斯再次入侵烏克蘭之間的持續不斷的間諜活動。

俄羅斯在烏克蘭損耗了大量軍事裝備，嚴重消耗了其巡航導彈和彈道導彈的軍械庫。隨著新制裁的實施和日益嚴格的出口管制，俄羅斯政府嘗試了通過進口替代來解決關鍵零部件被切斷供應的問題。這種方法後來被證明不可行。因此，俄羅斯現在亦或設計出新一代的但能力也許更弱的武器，亦或設法逃避制裁 ，這已成為其特別事務部門的一個關鍵任務。

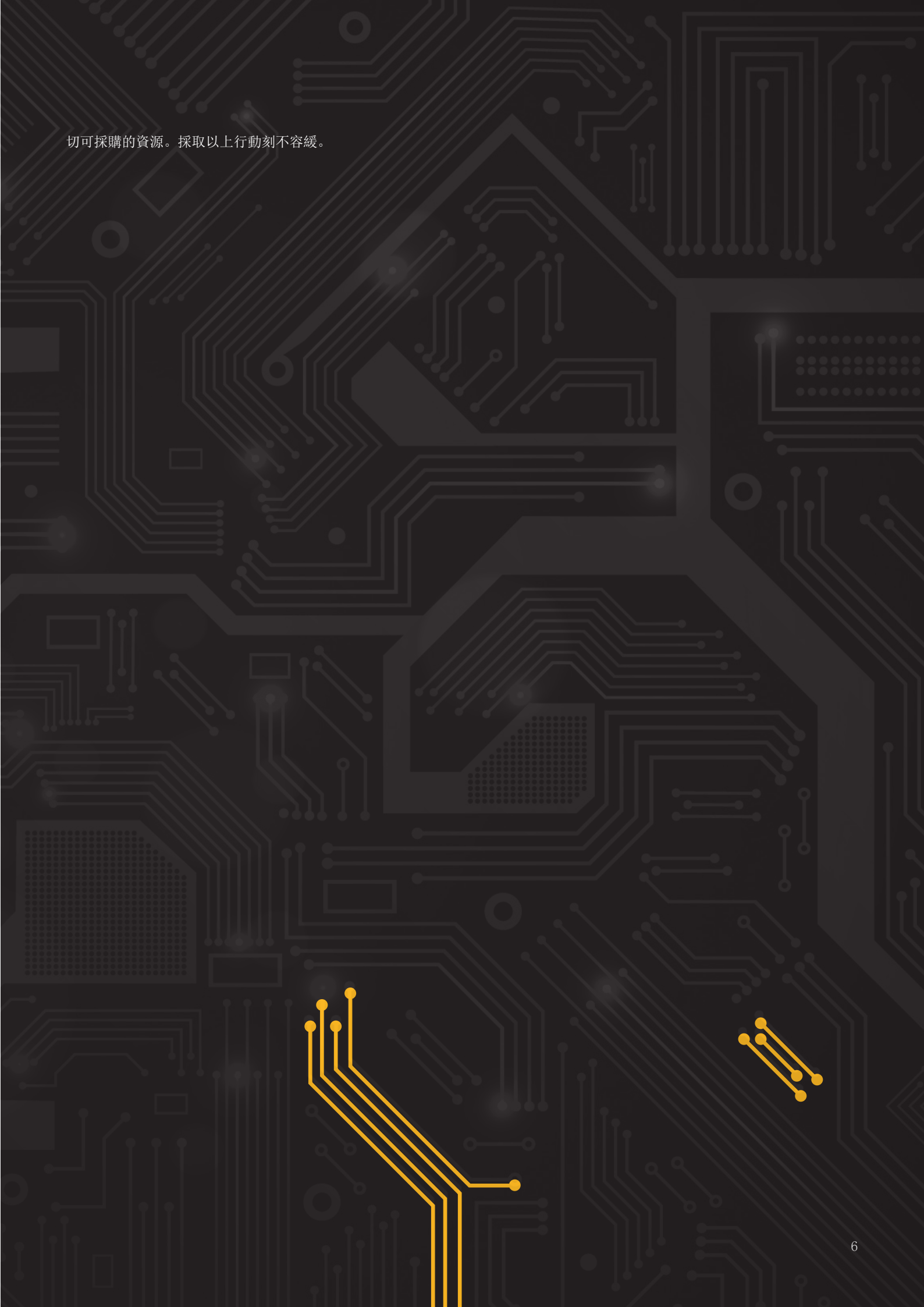
RUSI的分析表明，由俄羅斯特別事務部門運作的第三國轉運樞紐和秘密網絡目前正在努力建立新的供應路線，以確保能夠繼續採購西方的微電子產品。數年來，俄羅利用其運作的各種網絡——包括一系列幌子公司、欺詐性終端用戶許可證和其他蘇聯前輩創建的久經考驗的有效伎倆，在歐洲和北美洲非法採購。但俄羅斯也依賴了位於香港等轉運樞紐地的大型微電子分銷商的協助。近年來，這些分銷商不斷地往俄羅斯運送大量貨物。

要切斷俄羅斯這條矽生命線，各國政府必須做好以下工作：

- 審查並加強其本國和轄區內的現有出口管制。
- 開展多邊合作，查明並取締俄羅斯的秘密採購網絡。
- 防止 敏感微電子技術在支持俄羅斯的國家 獲得許可證而得以製造這些產品。
- 阻止第三國和管轄區向俄羅斯轉口或轉運受管制貨物。

俄羅斯正爭分奪秒地在網絡被取締前大肆採購一

切可採購的資源。採取以上行動刻不容緩。



引言

「是的，在過去的幾年裡，我們確實還沒能在進口替代領域解決一切難題.....。但大可不必過於擔心，因為在那些能確保我們主權的關鍵領域，我們已經做好了必要的工作。」.[1]

鏡頭中是一個烏克蘭小鎮的廣角景象。一架Orlan-10無人機的獨特十字線佔據了屏幕的中心。它是一種俄羅斯偵察無人機，用於協調炮擊行動。操作員放大各種各樣的卡車的圖像；可以看到烏克蘭方的人員聚集在卡車周圍。

錄像機是由索尼公司製造的，被安裝在美國Hextronik公司製造的萬向節電機上。它的縮放功能操作起來平穩，目標識別非常清晰。Orlan-10的飛行控制系統能使其始終保持在目標上方，因為它採用了瑞士一家名為意法半導體公司（STMicroelectronics）製造的STM32F103VC微控制器。該無人機由日本公司Saito Seisakusho的發動機驅動。正是這些零部件讓Orlan-10成為一架作戰範圍可達120公里的可靠飛行器。Orlan-10的導航芯片是u-blox Neo-M8 GNSS模塊，於2018年首次在Orlan-10上亮相。[2]UAV的坐標可能是通過亞德諾半導體技術有限公司（Analog Devices）製造的射頻敏捷收發器傳達給其操作員。

Orlan-10操作員在確認影像後，會計算出目標的坐標，以便向負責火力的控制總部提供準確的位置數據。一旦確定了坐標，目標數據就會被轉發給無線電操作員，操作員通過VHF R-168 Akveduk無線電台再將目標數據傳達給砲兵旅的指揮和控制基礎設施，以建立殺傷鏈。

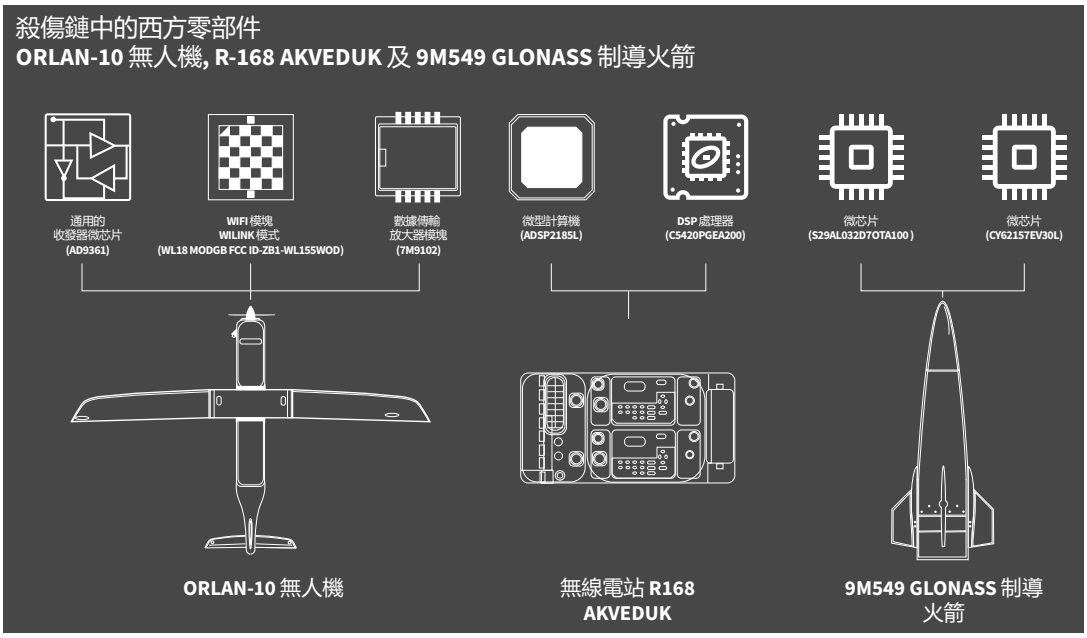
1 Izvestiya,[普丁在歐亞經濟論壇上的講話], 2022年5月26日, <https://iz.ru/1340365/video/vystuplenie-vladimira-putina-na-evraziiskom-ekonomicheskom-forume>, 訪問日期2022年7月18日。[作者俄語翻譯: 'Da, konechno, ne vse udalos' sdelat' za predyduschie gody v oblasti importzamescheniya… No eto nichego zdes' strashnogo net: po klyuchevym napravleniyam, kotorye obespechivayut nash suverenitet, my sdelali samoe neobhodimoe']. 這些言論是在歐亞經濟論壇上發表講話時發表的，該論壇主題為俄羅斯工業為應對西方制裁所做的努力。這裡的「主權」一詞可能是指俄羅斯的經濟獨立，而不是領土主權。

2 Inform Napalm, 「俄羅斯無人機Orlan-10由美國和其他國家製造的零部件組成——照片證據」, 2018年6月2日, <https://informnapalm.org/en/russian-drone-orlan-10-consists-of-parts-produced-in-the-usa-and-other-countries-photo-evidence/>, 訪問日期2022年7月18日 。

由Sarapul無線電廠[3]建造的R-168 Akveduk上用到了十幾個由西方公司製造的零部件。無線電的控制板上安裝了一個由美國亞德諾半導體科技公司製造的微控制器和一個由美國德州儀器公司（Texas Instrument）製造的數字信號處理器。操作員的聲音通過發射板被編碼並傳遞到殺傷鏈上，發射板上也裝有西方的多個零部件以及一家韓國公司製造的鎖相迴路（PLL）矽柵。

火力任務由「龍捲風-S」多管火箭發射器炮台完成，這是一套搭載了GLONASS衛星導航系統的相對較新的系統。[4] 在這一火力任務中，該炮台將採用300-mm 9M549 GLONASS制導火箭彈。據報導，該火箭的射程為120公里，圓概率偏差為7-15米。[5] 300毫米火箭搭載了一部複雜的計算單元連同一套三軸光纖陀螺儀和衛星導航信號處理單元，使彈藥的航向可在飛行中被修正，確保以更大的精度在更大的範圍內打擊更小的單一目標。火箭的陀螺儀採用了阿爾特拉公司（Altera Corporation）製造的現場可編程門陣列（FPGA），而其衛星導航信號處理和計算單元都依賴於賽普拉斯半导体公司（Cypress Semiconductor）製造的高速靜態隨機存取存儲器（SRAM）模塊。

Figure 1: 俄羅斯殺傷鏈中由西方設計和製造的零部件



來源： RUSI.

火箭發射後，Orlan-10將保持目標影像，並將目標位置的所有變化向炮組報告。然後不斷修正並反饋給殺傷鏈，且最終在飛行途中反饋給火箭的計算單元，以確保達到最致命效果。在這一實例中，Orlan-10操作員在他們的屏幕上觀察其打擊力：可以看到至少兩輛卡車被炸毀，幾名烏克蘭人員被殺。

這是RUSI重建的殺傷鏈，自俄羅斯2014年和2022年入侵烏克蘭以及2015年介入敘利亞以來，這種假設在現實世界中已经以各種形式，在各种迭代中重复上演了数百次，甚至數千次。但是，如果沒有西方的關鍵零部件和电子产品的支持，這些是不可能發生的。

3 Army Guide, ‘SARAPUL RADIOPLANT OJSC’, <http://www.army-guide.com/eng/firm1087.html>, 訪問日期2022年7月18日。

4 Tracy Cozzens, 「俄羅斯測試新的GLONASS制導導彈」, GPS World, 2020年9月22日, <https://www.gpsworld.com/russia-tests-new-glonass-guided-missile/>, 訪問日期2022年7月18日。

5 N R Jenzen-Jones及Charlie Randall, 「（2022年）在烏克蘭記載的俄羅斯9m54系列貨運導彈」, 軍備研究處, 2022年3月6日, <https://armamentresearch.com/russian-9m54-series-cargo-missile-documented-in-ukraine-2022/>, 訪問日期2022年7月18日。

以上描述的武器系統在俄羅斯軍事行動中絕非特例，俄羅斯的武器系統和軍事平台中常安裝了一系列主要從西方採購的零部件和電子設備，它們對這些系統和平台的功能起着關鍵性作用。克里姆林宮的戰爭機器——從火箭系統到彈道導彈，從戰術無線電到電子戰平台，通常情況下都依賴國外採購的零部件。

本報告對迄今為止在開源資料中尚未發布的最全面的零部件數據集進行分析，詳盡地揭示了俄羅斯軍隊如何依賴西方技術的事實。

數據集包括自2022年2月入侵以來在烏克蘭尋獲的從俄羅斯武裝部隊繳獲或由其消耗的近30種武器系統、平台和設備。在某些情況下，RUSI工作人員在烏克蘭各地實地檢查了這些武器。有些武器屬於老系統，可能是幾十年前在蘇聯時代終結時建造的。而其它是在近些年製造的最先進的平台，得益於俄羅斯耗費數十億美元的軍事現代化計劃。

但無論這些武器製造於什麼年代和日期，它們都有一個共通點：即，俄羅斯的武器（從標準武器到精品武器），都大量採用了在北美、歐洲和東亞原始製造的微電子元件。雖然俄羅斯武裝部隊能夠比較容易地從國內或國際批發商處購買其中的成品商用零部件等，但其它零部件則可能是通過俄羅斯對外情報局（SVR）或俄羅斯軍事情報總局（GRU）運作的秘密網絡採購得來的。

俄羅斯對烏克蘭的明目張膽的侵略行為可能使這一結論令人不安，但克里姆林宮開展的大量的科學與技術（S&T）間諜行動以及非法採購西方零部件確實不是什麼新鮮事。近一個世紀來，俄羅斯情報部門一直將收集科技信息和為俄羅斯的武器計劃獲取關鍵技術視為其工作的重點。[6] 蘇聯一心想要與西方國家制衡，因此，其技術間諜活動和用於處理這些信息的基礎設施非常龐大，隸屬於蘇聯研究機構的信息部門達1.1萬個，從業人員達10萬人。[7]

據RUSI分析，這些工作重點很可能從未改變過，因為SVR和GRU一直在積極採購所需的零部件以及技術知識，以便其能夠設計和製造旨在粉碎對手的武器。

繼2022年2月入侵烏克蘭後，克里姆林宮遭遇了對其實施的全方位的新制裁。此時的克里姆林南宮既要設法找到新零部件來替代，同時又要建立將零部件運入俄羅斯的替代供應鏈，這絕非易事。俄羅斯已損耗了大量的高端武器系統和平台，其軍工複合體需要獲得大批新零部件來維持其作戰行動，並為其武裝部隊的未來作戰提供裝備。

俄羅斯政府最高層人員當然深知這一問題。因此多年來，克里姆林宮一直在推動進口替代，以抵消西方製裁帶來的負面影響，但是收效甚微。[8] 2014年6月，弗拉基米爾　普丁強調了進口替代對俄羅斯軍隊的重要性，並呼籲廣泛領域地過渡到採用國產軍事零部件。[9] 然而，時隔八年，俄羅斯在啟動半導體本土化革命方面似乎並未取得有效進展，而旨在削弱俄羅斯軍工複合體能力的多邊制裁使得這一願望現在幾乎不可能實現。

虽然俄羅斯武器的有些零部件可以從中國采購，但無法獲得許多關鍵的零部件。如果沒有必要的國內製造能力，俄羅斯及其武裝力量仍然極易遭受多邊在切斷供應方面的努力的影響，其在烏克蘭的侵略成本也會更高。

6 美國中央情報局，「跨部門情報備忘錄：蘇聯情報部門獲取技術的努力」，1982年6月18日。另參閱Kevin Riehle，俄羅斯情報（Bethesda，MD：國家情報大學，2021年），第81頁。

7 美國中央情報局，「跨部門情報備忘錄」，第7頁；Riehle，俄羅斯情報，第138頁 – 140頁。

8 如需了解更多關於俄羅斯在進口替代方面的努力，請參閱Tatyana Mischenko，'Podderzhali otechestvennogo proizvoditelya。Chto takoe importzamescheniye，kak ono prohodit v Rossii'［「支持國內製造商。什麼是進口替代？它是如何在俄羅斯實施的？」］，SovkomBlog，2022年1月27日，<https://sovcombank.ru/blog/umnii-potrebitel/podderzhali-otechestvennogo-proizvoditelya-chto-takoe-importozamescheniе-kak-ono-prohodit-v-rossii>，訪問日期2022年7月18日。

9 Interfax，「Putin zayavil o neobhodimosti uskorennogo perehoda promyshlennosti k importzamescheniyu」［「普丁表示行業需要加快向進口替代過渡」］，2014年7月28日，<https://www.interfax.ru/business/388216>，訪問日期2022年7月18日。

第 1 部分

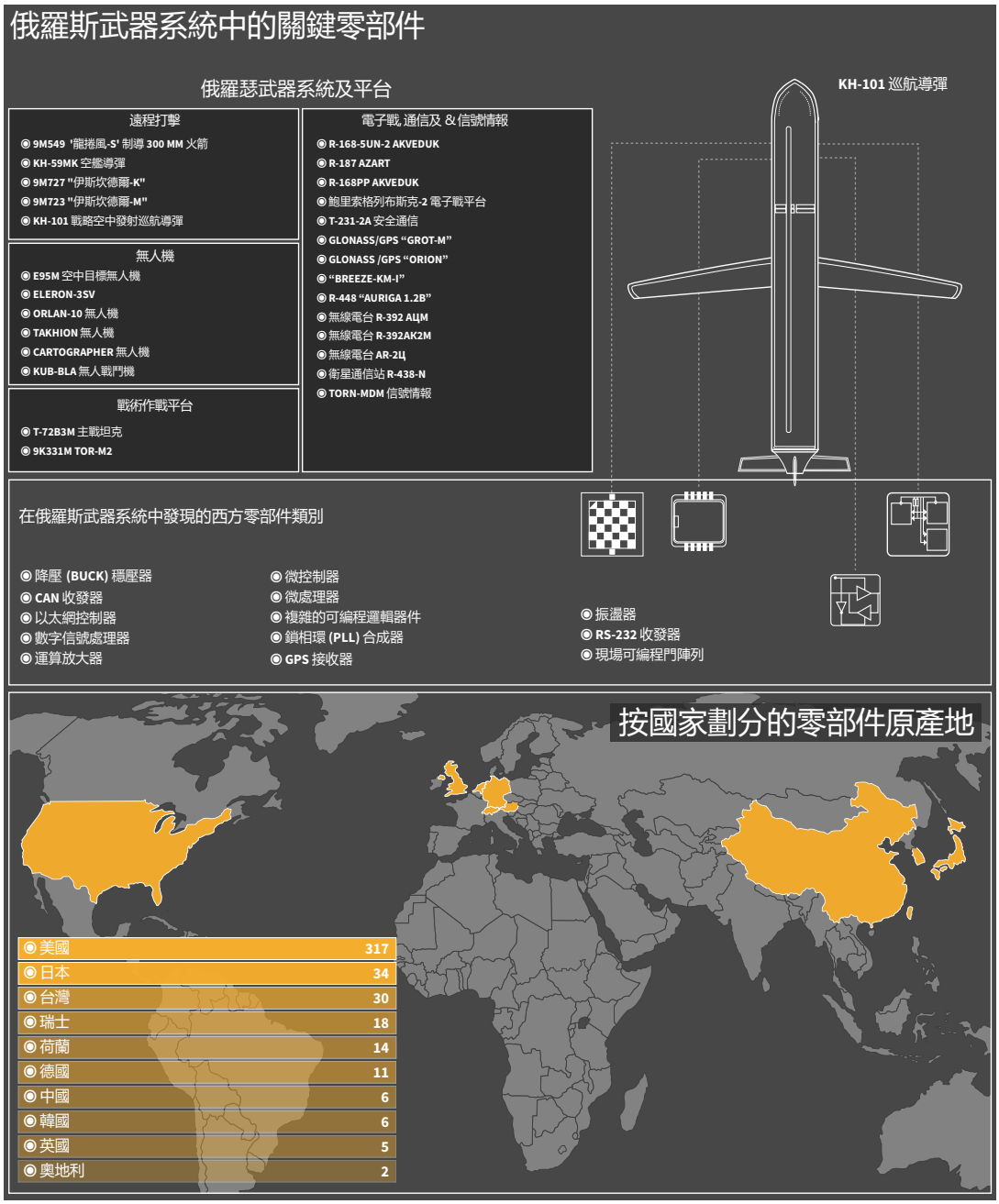
武器系統與西方零部件

RUSI獲得的數據涵蓋了自2022年2月俄羅斯全面入侵開始至6月底在烏克蘭尋獲或被消耗的27個武器系統、平台、無線電和設備組件。這些系統包括一些遠程攻擊裝備，如9M720伊斯坎德爾-M半彈道導彈，[10] 由伊斯坎德爾運輸機發射器（TEL）發射的9M727地射巡航導彈（GLCM）和 Kh-101戰略空射巡航導彈（ALCM）。還包括戰術戰鬥平台，如9K331M Tor-M2防空系統和各種無人機，無線電和衛星通信系統，如R-168 Akveduk戰術無線電，以及電子戰（EW）和信號情報（SIGINT）平台，如Torn-MDM。

10 半彈道導彈在很大程度上是彈道導彈，但能夠在飛行過程中進行機動操作，而且通常具有較短的射程。

01

Figure 2: 系統和零部件概述



來源：RUSI。

有些系統被找到時還完好無損。但有些情況下，特別是當彈道導彈和巡航導彈等彈藥已用完，找到的武器只能是不完整的，那麼這些武器的零部件情況就不一定構建得完整。因此，此處介紹的幾個系統的零部件列表不應被視作詳盡無遺。儘管存在局限，如此大規模地尋獲和拆卸這些系統為我們提供了一個前所未有的機會，幫助我們了解了這些武器是如何設計、製造並被部署到戰場上的。

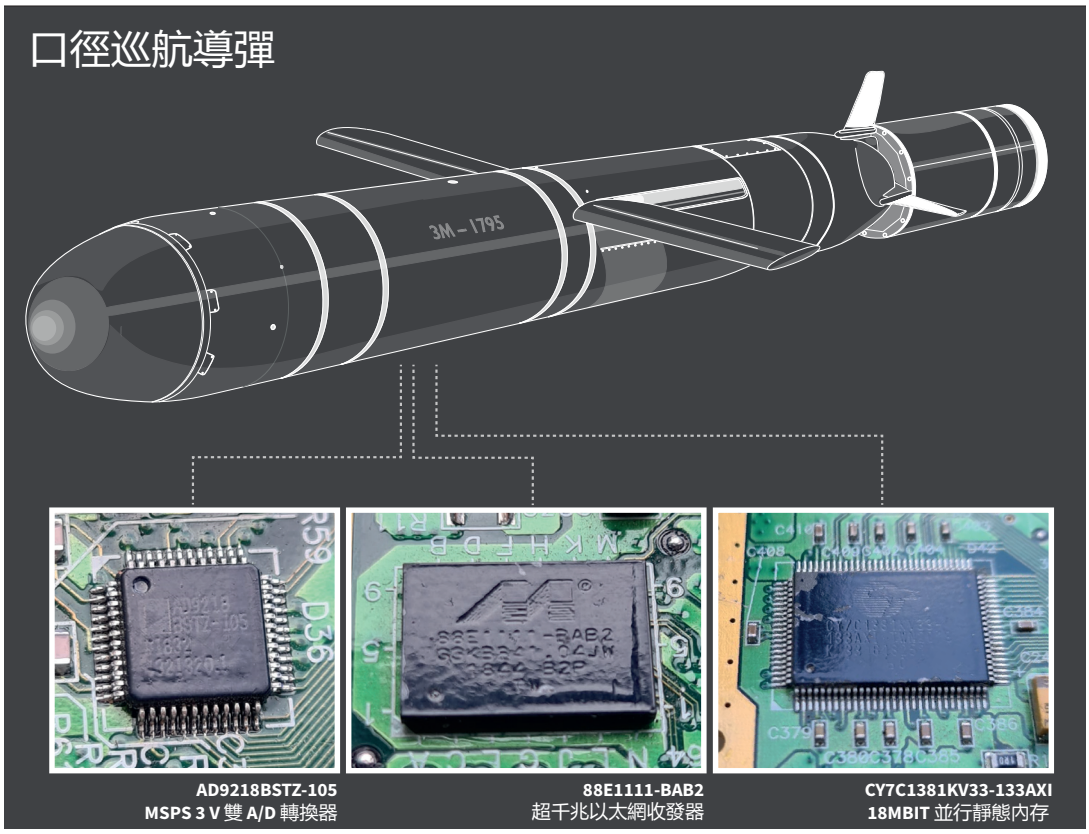
所有這些系統都使用了大量的西方設計的零部件，包括微電子、專用相機和傳感器、收發器和轉換器、空氣葉片、電機和一系列其它零部件。RUSI從中找出了450個主要來自西方製造商的獨特零部件，其中至少318個來自美國公司。有時，系統用到了幾個相同的零部件。而有時，相同的零部件出現在多個系統和子系統中，這意味著零部件的總數應高得多。

其中許多零部件都是平淡無奇的微電子產品，可以從很多國家和司法管轄區的在線分銷商處購買。而也有很多是為了防止其被用於軍事目的

而長期以來一直被限制出口的。繼克里姆林宮入侵烏克蘭後，絕大多數產品如今都已被限制出口到俄羅斯，尤其是那些軍事終端用戶所採購的產品。

零部件和微電子產品的製造日期各不相同。雖然有些是早在1980年代初就製造的，也可能是在那個時候採購來的，但有些卻是在最近幾年製造的。例如，在Kalibr巡航導彈中發現的西方設計的零部件似乎可以追溯到2018年和2019年，即在克里姆林宮入侵烏克蘭後，針對俄羅斯軍事終端用戶實施的廣泛制裁和出口管制的四年後。

Figure 3: Kalibr 巡航導彈現代零部件



來源：RUSI.

然而，不論零部件具體屬於哪個類別，俄羅斯如此大規模地使用西方製造的微電子和其它零部件，這本身就充分顯示了俄羅斯本土製造或從他國採購類似產品都一直進行得差強人意。這也突顯了自入侵烏克蘭以來，特別是對軍民兩用貨物和關鍵零部件出口管制方面的多邊努力，讓俄羅斯軍工複合體在更換損耗設備和材料方面舉步維艱。

全球採購

數據集中的大部分零部件來自57家美國公司。其中，最多見的是由一些領先的微電子製造商製造的，如亞德諾半導體技術有限公司（Analog Devices Inc）、德州儀器（Texas Instruments）、美信集成產品（Maxim Integrated），[11] 賽靈思（Xilinx Inc），[12]

11 自2021年8月起作為亞德諾半導體技術有限公司的子公司運營。參閱亞德諾半導體技術網頁，「亞德諾半導體技術成功收購美信集成產品公司」，新聞稿，2021年8月26日，<https://www.analog.com/en/about-adi/news-room/press-releases/2021/8-26-21-adi-completes-acquisition-of-maxim-integrated.html>，訪問日期2022年7月18日。

12 2022年2月被超微半導體（Advanced Micro Devices Inc）收購。參閱超微半導體網頁，「AMD 成功收購賽靈思（Xilinx）」，新聞發布，2022年2月14日，<https://ir.amd.com/news-events/press-releases/detail/1047/amd-completes-acquisition-of-xilinx>，訪問日期2022年7月18日。

微晶片科技（Microchip Technology Inc），安森美（ON Semiconductor），阿爾特拉（Altera Corporation），[13] 英特（Intel Corporation），愛特梅爾（Atmel Corporation）[14] 及賽普拉斯半導體（Cypress Semiconductor）。[15] 從俄羅斯武裝部隊使用的上述系統中的26個系統中，總共找到了208個由這10家公司製造的獨特零部件。

除了這些美國公司外，另外77個零部件分別由日本、台灣、韓國、中國和新加坡的公司設計和製造。其中13個由日本村田製作所（Murata Manufacturing Co Ltd）製造，7個由台灣國巨公司（Yageo Corporation）製造。

至少找到了55個來自歐洲公司的獨特零部件。值得注意的是，來自總部位於荷蘭的恩智浦半導體（NXP Semiconductors NV）和總部位於瑞士的意法半導體（STMicroelectronics）的產品佔最多數量。其他製造商還包括瑞士的u-blox、德國的愛普科斯（EPCOS）、法國的達利斯（Thales Group），以及總部位於英國的公司CML Microcircuits和Golledge Electronics。

雖然這些零部件中的大多數都有可供驗證和辨析出其製造商的序列號，但有一小部分序列號在製造商網頁上無法識別，可能已被停產。此外，還有部分零部件因可識別信息不充分，無法對其作出肯定的鑑定。還應該指出的是，零部件偽造是一種越來越普遍的現象，因此某些零部件也有可能是在其它地方製造的假冒偽劣品。

我們按照類型和子類型對這些零部件進行了分類，以方便理解這些俄羅斯系統中最常用的組成部分。最常見的是微控制器和微處理器，以及復雜的可編程邏輯器件 (CPLD) 和現場可編程門陣列（FPGA），它們能讓客戶和工程師們對製造完的集成電路自行配置。[16]

其它常見的西方製造零部件還包括 PLL 合成器、運算放大器、振盪器、RS-232 收發器、CAN 收發器、降壓穩壓器、以太網控制器、模數 (A/D) 轉換器和熱像儀。

雖然這類設備在商業電子系統中有着各種各樣的用途，但它們也決定着現代戰爭的進行方式。複雜的傳感器、信息處理系統、目標和導航複合體、加密通信設備和許多其它現代平台的功能的實現，都依賴於這些微電子設備。正因如此，渴求得到技術的俄羅斯軍工複合體會始終將這些零部件的製造、採購作為其優先事項來抓。

13 2015年12月被英特爾（Intel Corporation）收購。參閱英特爾新聞編輯室，「‘英特爾成功收購阿爾特拉」，新聞稿，2015年12月28日，<https://newsroom.intel.com/news-releases/intel-completes-acquisition-of-altera/#gs.5eb5ck>，訪問日期2022年7月18日。

14 2016年被微晶片科技（Microchip Technology）併購。參閱Claudia Assis，「微晶片科技以35.6億美金的價格收購芯片製造商愛特梅爾（Atmel）」，市場觀察，2016年1月19日。<https://www.marketwatch.com/story/microchip-technology-buys-chip-maker-atmel-in-356-billion-deal-2016-01-19>，訪問日期2022年7月19日。

15 2020年4月被英飛凌科技股份有限公司（Infineon Technologies AG）收購。英飛凌科技股份有限公司網頁，「英飛凌科技股份有限公司成功收購賽普拉斯半導體」，新聞稿，2020年4月16日，<https://www.infineon.com/cms/en/about-infineon/press/press-releases/2020/INFXX202004-049.html>，訪問日期2022年7月18日。

16 這些設備還需要用到編程設備，以便用戶在開發過程中或在工廠進行配置。而這些通常由芯片製造商銷售的編程設備則會用到許多可能受到出口管制的複雜的零部件。這意味著用戶想要導入CPLD和FPGA，還必須導入這些支持工具才能正確編程。賽靈思，「現場可編程門陣列 （FPGA）」，<https://www.xilinx.com/products/silicon-devices/fpga/what-is-an-fpga.html>，訪問日期2022年7月21日；techopedia，「複雜可編程邏輯器件 (CPLD)」，<https://www.techopedia.com/definition/6655/complex-programmable-logic-device-cpld>，訪問日期2022年7月21日。

堵住供應渠道：制裁與出口管制

自俄羅斯於2022年2月入侵烏克蘭後，美國、英國和歐盟通過了對俄羅斯的一系列全面製裁措施。[17] 其中包括針對金融和行業的製裁，以及旨在限制俄羅斯獲得軍事技術和關鍵零部件的一系列出口管制條例。[18] 日本、韓國、台灣、加拿大、澳大利亞和瑞士等許多其他國家和司法管轄區也承諾實施類似的出口管制。

儘管俄羅斯武器系統中發現的許多美國製造的零部件是在俄羅斯入侵烏克蘭之前根據出口管理條例（EAR99）已被獲准出口到俄羅斯的，但這些產品的美國出口商仍然有盡職調查義務，以確保它們的產品不被用於被制裁的終端用戶或最終用途。[19]

本報告涉及到的被檢查的俄羅斯武器中找到了一長串由美國公司製造的EAR99類零部件。德州儀器、亞德諾半導體技術、美信集成和賽靈思是它們的主要製造商，約佔總數的30%。值得注意的是，這些產品包括了對地理定位和計算至關重要的各種零部件，它們大致分四類：微控制器和微處理器、接口、放大器和 FPGA。

俄羅斯武器系統中存在着大量美國製造的EAR99類零部件，這就足以證明這些零部件亦或是從俄羅斯的經銷商處購買獲得的，亦或是從別處採購和轉運後用以軍事目的的。

在另外幾個實例中，從俄羅斯武器系統中發現的零部件甚至早在2022年2月入侵烏克蘭前就已經受到了更嚴格的出口管制。[20] 不僅僅美國製造的零部件，[21] 其它地方（如英國、歐盟、日本、韓國和台灣）製造的通常也是這種情況。這意味着這些零部件很可能是在入侵之前的某些時候通過非法採購後被秘密運往俄羅斯或被欺詐性轉運至軍事終端用戶的。

2007年被洩露的幾份電報顯示，美國政府內部對向俄羅斯出口受管制物品進行了審議。其中涉及亞德諾製造的A/D轉換器，該轉換器與在烏克蘭的幾個武器系統中發現的非常相似。[22] 儘管俄羅斯進口商最終被判定為民用實體，但直接出口受管制美國技術是需要許可證的，在裝運後還可能需要經檢查確認該產品用於非軍事目的。[23]

但在俄羅斯於2014年入侵和吞併克里米亞之後，一系列國家已經開始嘗試限制向俄羅斯軍工複合體的零部件供應。2014年初，美國工業和安全局（BIS）擴大了對俄羅斯的出口限制，所有向俄羅斯或克里米亞出口或再出口任何有助於俄羅斯或克里米亞軍事能力或國防工業基地的高科技物品的未決許可證申請都遭到了拒絕。[24] 同年7月，歐盟也開始效仿並實施制裁，其中包括禁運武器及其相關材料，以及禁運用於軍事用途或軍事終端用戶的軍民兩用商品和技術產品。[25]

17 有關英國的措施，請參閱英國外交、聯邦和發展辦公室 （FCO）2022年7月19日發布的《英國對俄羅斯的製裁》，<https://www.gov.uk/government/collections/uk-sanctions-on-russia>，於訪問日期2022年7月20日；有關美國措施，請參閱美國財政部，「烏克蘭-/俄羅斯相關製裁」，<https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/ukraine-russia-related-sanctions>，訪問日期2022年7月20日訪問；有關歐盟措施，請參閱歐盟委員會，「俄羅斯對烏克蘭發動軍事侵略後採取的製裁措施」，<https://ec.europa.eu/info/business-economy-euro/banking-and-finance/international-relations/restrictive-measures-sanctions/sanctions-adopted-following-russias-military-aggression-against-ukraine_en>，訪問日期2022年7月20日。

18 Ibid.

19 美國商務部國際貿易管理局，「出口管制分類號（ECCN）和出口管理條例（EAR99）」，<https://www.trade.gov/eccn-and-export-administration-regulation-ear99>，訪問日期2022年7月18日。

20 本項目的零部件與公開資料進行了交叉對比，以確定它們是否屬根據ECCN或EAR99規則分類。請參閱「方法」。

21 使用美國原產技術的外國製造零部件超過一定程度的仍將受到美國出口管制，並可能需要出口許可證。請參閱美國商務部工業和安全局，「視作出口常見問題解答 – 哪些技術受商務部管制？」，<https://www.bis.doc.gov/index.php/policy-guidance/deemed-exports/deemed-exports-faqs/faq/48-what-technologies-are-subject-to-the-commerce-department-controls>，訪問時間2022年7月25日。

22 維基解密，「EXTRANCHECK：許可前檢查：JSC VREMYA- CH, NIZHNY NOVGOROD, 俄羅斯，許可證號D368426」，2007 年1月12日，<https://wikileaks.org/plusd/cables/07MOSCOW86_a.html>，訪問日期2022年7月19日。

23 美國商務部國際貿易管理局，「出口管制分類號（ECCN）和出口管理條例（EAR99）」。<https://www.trade.gov/eccn-and-export-administration-regulation-ear99>，訪問日期2022年7月18日。

24 美國商務部工業和安全局，「商務部宣布擴大對俄羅斯的出口限制範圍」，新聞稿，2014年4月28日，<https://www.bis.doc.gov/index.php/all-articles/107-about-bis/newsroom/press-releases/press-release-2014/665-commerce-dept-announces-expansion-of-export-restrictions-on-russia>，訪問日期2022年7月19日。

25 歐盟理事會，「時間表——歐盟就俄羅斯入侵烏克蘭針對俄羅斯採取的管制措施」，<https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/history-

此後，美國逐漸擴大了出口限制的範圍。例如，2020年12月,BIS發布了一份包含58家中國和45家俄羅斯公司的「軍事終端用戶」（MEU） 清單，要求出口商、再出口商和想在國內轉移零部件的公司必須先獲得出口許可證，方可將EAR產品轉移到清單上這些實體。[26]

2021年3月，BIS還大幅縮小了EAR許可證豁免的範圍，暫停了涉及因國家安全原因而被管制的、運往俄羅斯的物品交易，包括許可證豁免RPL（即組件和設備的維護和更換）、許可證豁免TSU（不受限制的技術和軟件）和許可證豁免 APR（額外允許再出口）。[27]

BIS實體清單

自2022年俄羅斯入侵烏克蘭以來，BIS已將大量俄羅斯和白俄羅斯公司添加到其實體清單中，實體清單是一份貿易限制清單，名單上包含了受EAR兩用物品管理辦法管制的外國人員、實體和政府。[28] 名單所列各方參與的活動亦或受到美國國務院的製裁，亦或違反美國的國家安全或外交政策利益。[29]

實體清單要求名單上的實體（無論EAR其它部分對許可有何要求）必須獲得許可。針對其中一些名單實體，即使是歸類為EAR99的商品也需要出口商獲得許可證後方能將其出口、再出口或（在國內）轉移給該方。[30] 雖然不像被列入BIS的「未經核實清單」或被指定為「被拒絕方」那樣嚴格，但對於實體清單上的大多數實體，BIS實施了假設拒絕的許可審查政策，有效地阻止了那些清單上實體接收美國出口商分類編號（ECCN）和EAR99兩用商品的情況。

因此，儘管大規模製裁和出口管制收緊可能會嚴重削弱俄羅斯為其武器採購西方零部件的能力，但該國武器平台中發現的許多零部件卻早在2014年和2022年俄羅斯入侵前就已經受到管制。[31]

事實上，在俄羅斯武器系統中發現的總共81種獨特零部件被歸類為兩用物品，並在美國政府的商業管制清單上有相應的出口管制分類編號 (ECCN)。[32] ECCN系統使用五個字符的字母數字名稱來確認商品是否需要美國商務部的出口許可證。如果商品帶ECCN，則該產品已被歸類為兩用商品，出口商必須獲得此許可證才能運往國外。

---

restrictive-measures-against-russia-over-ukraine/>, 訪問日期2022年7月19日。

26 美國商務部工業和安全局，「第744部分的第4號補充 – 實體清單」，2022年6月28日， <https://www.bis.doc.gov/index.php/documents/regulations-docs/2326-supplement-no-4-to-part-744-entity-list-4/file>，
訪問日期2022年7月19日。

27 Alexandre (Alex) Lamy、Lise S Test和Paul Amberg，「BIS和DDTC加強美國對俄羅斯的出口管制，作為對Navalny中毒和被監禁事件的回應」，制裁和出口管制更新，2021年3月29日，<https://sanctionsnews.bakermckenzie.com/bis-and-ddtc-implement-strengthened-us-export-controls-on-russia-in-response-to-poisoning-and-imprisonment-of-navalny/>, 訪問日期2022年7月19日。

28 美國商務部工業和安全局，「實體清單」，<https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list>，訪問日期2022年7月19日。

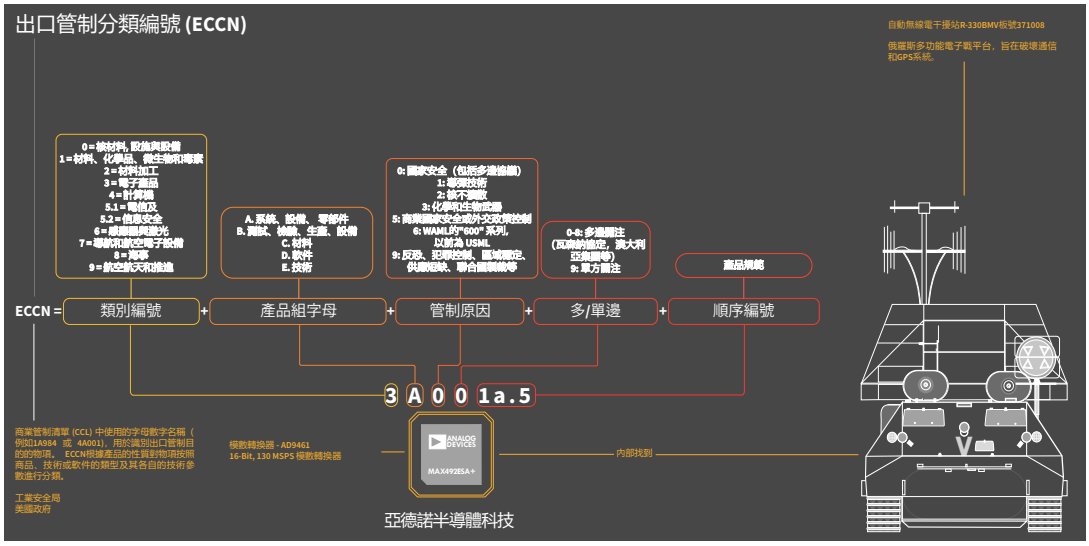
29 Ibid.

30 Ibid.

31 美國商務部工業和安全局，「商業管制清單 (CCL)」， <https://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl>，訪問日期2022年7月19日。

32 本調查涉及的零部件與公開資料進行了交叉對比，以確定它們是否屬根據ECCN或EAR99規則分類。請參閱「方法」。

Figure 4: 了解出口管制分類編號



來源：美國工業和安全局；麻省理工學院出口管制，「出口管制分類編號（ECCN）指南」；RUSI。

在俄羅斯最關鍵的武器系統中發現了許多這些美國製造的受管制零部件，例如9M549 300毫米GLONASS制導火箭、Kh-59反艦導彈（AShM）和R-330BMV電子戰系統。9M549火箭和Kh-59安裝ECCN閃存和SRAM模塊。同時，R-330BMV上安裝了各種ECCN管制零部件，包括FPGA、CPLD、微處理器、數字信號處理器和A/D轉換器。

其它ECCN商品還包括Kh-101 ALCM上的荷蘭半導體和9M727 GLCM上的高性能CMOS靜態RAM芯片。在Torn-MDM SIGINT系統中還發現了五個ECCN零部件，包括西方製造的微控制器和射頻放大器。然而，含有最多ECCN零部件的系統通常是無線電設備。例如，R-392 ACM無線電裝有至少六個獨特的ECCN類零部件。

這些受管制商品中有很大一部分最初是由總部位於美國的公司製造的，佔數據集中ECCN商品的78%。總體上，俄羅斯武器系統中大約25%的ECCN類產品的原始製造商是亞德諾半導體技術和德州儀器。

ECCN類零部件的其它美國製造商包括英特爾、愛特梅爾、賽普拉斯半導體和微晶片科技。日本和台灣製造商分別以10件和9件產品緊隨其後，位居第二和第三。

美國頭號通緝犯

數十年來，俄羅斯情報機構及其蘇聯前身在其間諜活動和採購努力中，一直將其目標對準美國領先的計算機和微電子公司。1985年，美國政府對蘇聯收購目標的評估中將IBM和德州儀器確認為蘇聯的優先滲入目標。[33] 叛離者Vasili Mitrokhin公佈的克格勃檔案顯示，克格勃甚至早在1964年就設法在德州儀器的法國辦事處安插了一名間諜。[34] 但這些行動的驚人程度直到1981年才被暴露，當時為克格勃工作的蘇聯工程師Vladimir Vetrov向法國情報部門提供了4,000份關於X線（Line X）活動的秘密文件，X線是一個技術收集部門，是克格勃第一總局的T局。[35] 根據後來被命名為「告別檔案」的文件顯示，蘇聯的觸角幾乎無處不在，他們在世界各地僱用了100多名克格勃特工。[36] 該檔案還證明，這些特工成績斐然，從西方國家收集了大量的科技信息和資料。據報導，61.5%的科技間諜材料來自美國，10.5%來自西德，8%來自法國，7.5%來自英國，3%來自日本。[37]

33 國防部長辦公室，「蘇聯獲取具有重要軍事意義的西方技術：更新」，1985年9月，https://apps.dtic.mil/sti/pdfs/ADA160564.pdf>，訪問日期2022年7月19日。

34 Christopher Andrew 與 Vasili Mitrokhin, Mitrokhin 檔案 （倫敦：企鵝出版社，1999年），第245頁。

35 David G Major, 「告別」，1999, <https://cdn.ymaws.com/cicentre.com/resource/resmgr/articles/farewell_old_reason_by_david.pdf>，訪問日期2022年7月19日。

36 Ibid.

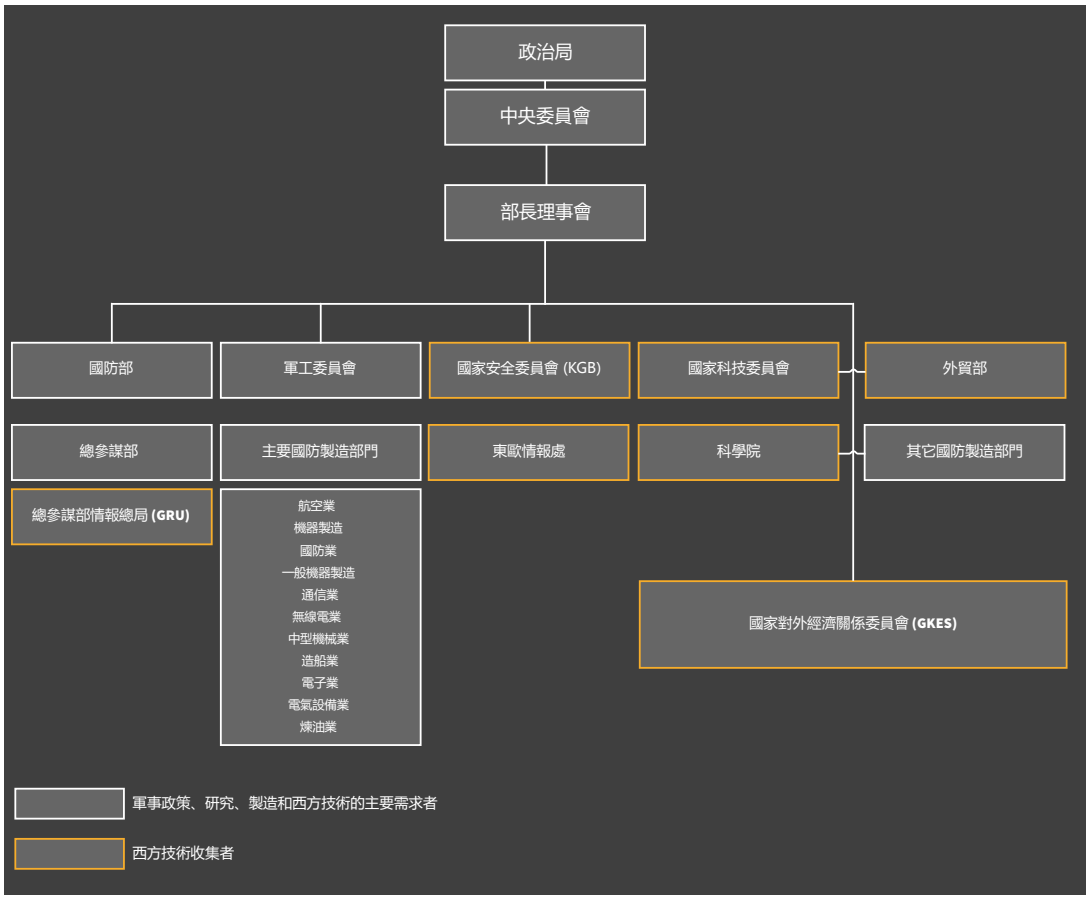
37 Christopher Andrew與Vasili Mitrokhin, Mitrokhin 檔案2《克格勃與世界》（The KGB and the World）（倫敦：企鵝出版社，2006年），第306頁。

X線的努力取得了令人矚目的成功。根據美國中央情報局（CIA）自己1982年的評估顯示，蘇聯獲得併「完全複製」了美國的AIM-9響尾蛇空對空導彈，該導彈為蘇聯帶來了首枚紅外制導導彈 Vympel K-13。[38] 響尾蛇只是數百個例子中的一例。蘇聯還獲得了其它導彈，例如肩射式FIM-43紅眼MANPADS便攜式系統、美國 LGM-30 Minuteman ICBM制導子系統的數據、固體推進劑導彈的數據、F-14、F-15、F-18戰鬥機上搭載的系統的雷達數據，和大量其它系統的信息。[39]

38 美國中央情報局，《跨機構情報備忘錄》，第9頁。關於蘇聯如何獲得AIM-9響尾蛇飛彈的另一種理論是，在1958年9月在台灣 F-86 Sabres 戰鬥機與中國MiG-17戰鬥機進行空中交戰時，一部未爆炸的AIM-9B落入了MiG-17 戰機鬥內。 據說後來整枚導彈被送到蘇聯進行逆向工程，隨後開發出了Vympel K-13型導彈。參閱美國科學家聯盟，「AA-2 ATOLL K-13（R-3或Object 310）PL-2 / PL-3 / PL-5」，https://web.archive.org/web/20160304041942/http://fas.org/man/dod-101/sys/missile/row/aa-2.htm>，訪問日期2022年7月20日。

39 美國中央情報局，《跨機構情報備忘錄》，第9頁。

Figure 5: 負責指導和採購西方技術的蘇聯實體



來源：Frank Dittmann, 《社會主義下的微電子》（Microelectronics under Socialism）; RUSI.

蘇聯的解體似乎只是暫時放緩了這些活動步伐。例如，2012年，有11人被指控經營走私團伙，試圖「主要為俄羅斯政府機構，包括俄羅斯軍事和情報機構」出口微電子等關鍵技術。[40] 根據當時的媒體報導，[41]走私團伙的目標是數家美國公司，包括德州儀器和亞德諾半導體技術公司，他們聲稱受到了為Arc Electronics工作的俄羅斯特工的欺騙，Arc Electronics是一家用於採購他們的產品並將其運回俄羅斯的幌子公司。[42] 美國司法部提交的文件稱，2002年至2012年間，Arc Electronics公司向俄羅斯國防部的軍事設備供應商運送了價值5000萬美元的商品。[43]

40 美國紐約東區地方法院，「美利堅合眾國對 Alexander Fishenko 等人」，起訴書，2012年9 月28日，<https://www.wired.com/images_blogs/dangerroom/2012/10/indictment.pdf>，訪問日期2022年7月20日。

41 Christie Smythe、Iain King和彭博新聞社，「美國稱德州儀器、賽靈思受俄羅斯出口集團欺騙」，華盛頓郵報，2015年9月26日。

42 Ibid.

43 美國司法部檢察官辦公室，「向俄羅斯軍方出口微電子產品的出口商在審判中因所有罪名被定罪後被判處135個月監禁」，2017年2月28日，<https://www.justice.gov/usao-edny/pr/exporter-microelectronics-russian-military-sentenced>，訪問日期2022年7月20日。

近幾個月來，美國政府還在繼續追查俄羅斯的秘密採購網絡。2022年入侵僅一個月後，美國財政部就點名了30多名個人和公司，指控這些個人和公司代表俄羅斯情報機構採購關鍵的西方技術。被點名的這些公司包括一個以俄羅斯實體Serniya Engineering為中心的網絡，美國財政部聲稱該實體在英國、馬耳他、新加坡、西班牙和俄羅斯指揮著一個複雜的公司網絡。[44]

Serniya Engineering據稱成立於2017年，[45] 而此前使用 Serniya Engineering 域名的公司NPO Sernia，過去與Serniya Engineering在同一域名下註冊，且列出的業務範圍相同。補充報告指出，NPO Sernia公司於2016年解散，[46] 而Serniya Engineering於2017年成立。

但是，這些時間表與其它開源報告不一致。Serniya Engineering網站的存檔實例顯示，[47] 該公司是在1998年左右成立的。2021年4月發表的文章指出，Serniya Engineering成立於1980年代後期，隸屬於莫斯科物理部門——即NPO Sernia多年來一直使用的地址。[48]

NPO Sernia網站的存檔頁面聲稱其一些重點項目是代表外交部和其他政府機構進行的。這些機構（包括聯邦安全局 (FSB) 和聯邦保護局 (FSO)）的標誌出現在2007年至2013年間的該公司網站上。[49]

44 美國財政部，「財政部瞄準制裁規避網絡和支持普丁戰爭的俄羅斯科技公司」，新聞稿，2022年3月31日，<https://home.treasury.gov/news/press-releases/jy0692>，訪問日期22年7月20日。

45 rusprofile, LLC 「Serniya Engineering」，上次更新2022年7月21日，<https://www.rusprofile.ru/id/10885594>，訪問日期 2022年7月23日。

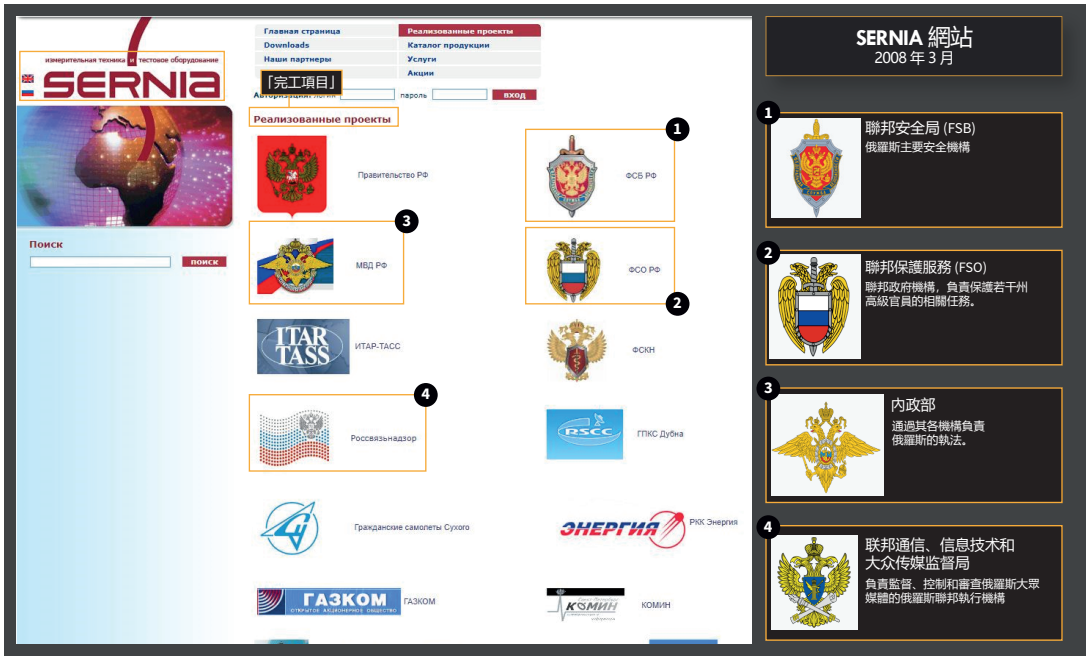
46 與Serniya Engineering溝通的《金融時報》報導指出，NPO Sernia公司已於2016年3月解散。參閱Jamie Powell，《Djeco Group到底是誰？》，《金融時報》，2022年3月25日。欲獲更多信息，請參閱<https://www.ft.com/content/63c80363-644d-4981-a144-c618144845e6>，訪問日期2022年7月22日。

47 2007年7月的存檔頁面，參閱Sernia.ru，「O Kompanii 」[關於公司]，可訪問 Wayback Machine 網頁，<https://web.archive.org/web/20070715005149/http:/www。 sernia.ru/?aux_page=about_company>，訪問日期2022年7月19日。

48 TMC，「對 Sernia Engineering員工的採訪」，<https://go.techmfg.com/l/910112/2021-04-29/9r31>，訪問日期2022年7月20日。

49 2013年7月的存檔頁面，請參閱Sernia.ru，「已完工項目」，通過Wayback Machine訪問，<https://web.archive.org/web/20130830145236/http://www.sernia.ru/relized_projects>，訪問日期2022年7月19日。另請參閱Powell的 《Djeco Group到底是誰？》。

Figure 6: Sernia的舊網站展示FSB和FSO標誌



來源： Serniya.ru; RUSI.

Serniya Engineering網絡的一個中心節點是位於俄羅斯的Sertal LLC。[50] 該公司網站上的公開地址位於莫斯科郊區一個不起眼的公寓樓， 宣傳自己是德州儀器、亞德諾半導體技術、賽普拉斯半導體、 恩智浦半導體、意法半導體和一系列其它公司製造的「電子零部件供應商」。[51] 值得一提的是，這些公司製造的零部件是在烏克蘭的俄羅斯武器平台上發現的數量最多的。

50 美國財政部，「財政部瞄準規避制裁網絡和支持普丁戰爭的俄羅斯科技公司」，新聞稿，2022年3月31日，<https://home.treasury.gov/news/press-releases/jy0692>，訪問日期22年7月19日。

51 Sertal.ru的存檔版鏈接為 <https://web.archive.org/web/20220000000000*/sertal.ru>，訪問日期22年7月19日。

Figure 7: 2022年2月Sertal的網頁

來源： Sertal.ru; RUSI.

裝運級的貿易記錄證實，Sertal確實運輸了這些類型的美國製造商品。例如，就在不久前的2021年3月，Sertal通過香港中介進口了價值60萬美元的德州儀器製造的電子集成電路。[52] 七個月後，該公司又從同一家香港出口商那裡進口了價值110萬美元的電子集成電路，這一次是由賽靈思公司製造的。[53]

大盜亞德諾

儘管俄羅斯長期以來一直努力培養本土半導體產業，但根據本報告分析的數據顯示，俄羅斯的武器配備了大量美國公司原產的零部件。其中最突出的兩家公司正是亞德諾半導體技術和德州儀器，都是製造專門用於國防應用的產品的微電子製造商。

事實上，在RUSI數據集中的450個獨特零部件中，亞德諾半導體技術和德州儀器製造的產品佔俄羅斯武器中發現的所有零部件的近四分之一。這些從一般到高度專業的零部件，都能在最關鍵的系統中被找到——例如彈道導彈和巡航導彈及其它精密彈藥和電子戰平台。

數據集總共包含亞德諾半導體技術公司製造的50個獨特零部件，其中13個根據美國法律被歸類為兩用商品，即出口商很可能需要獲得許可證才能將這些零部件出口到國外。它們主要是微處理器和微控制器，[54] 但也有移動通信設備、[55]電信傳輸設備[56] 和A/D轉換器。[57]

52 由第三方商業供應商提供的貿易數據。

53 Ibid.

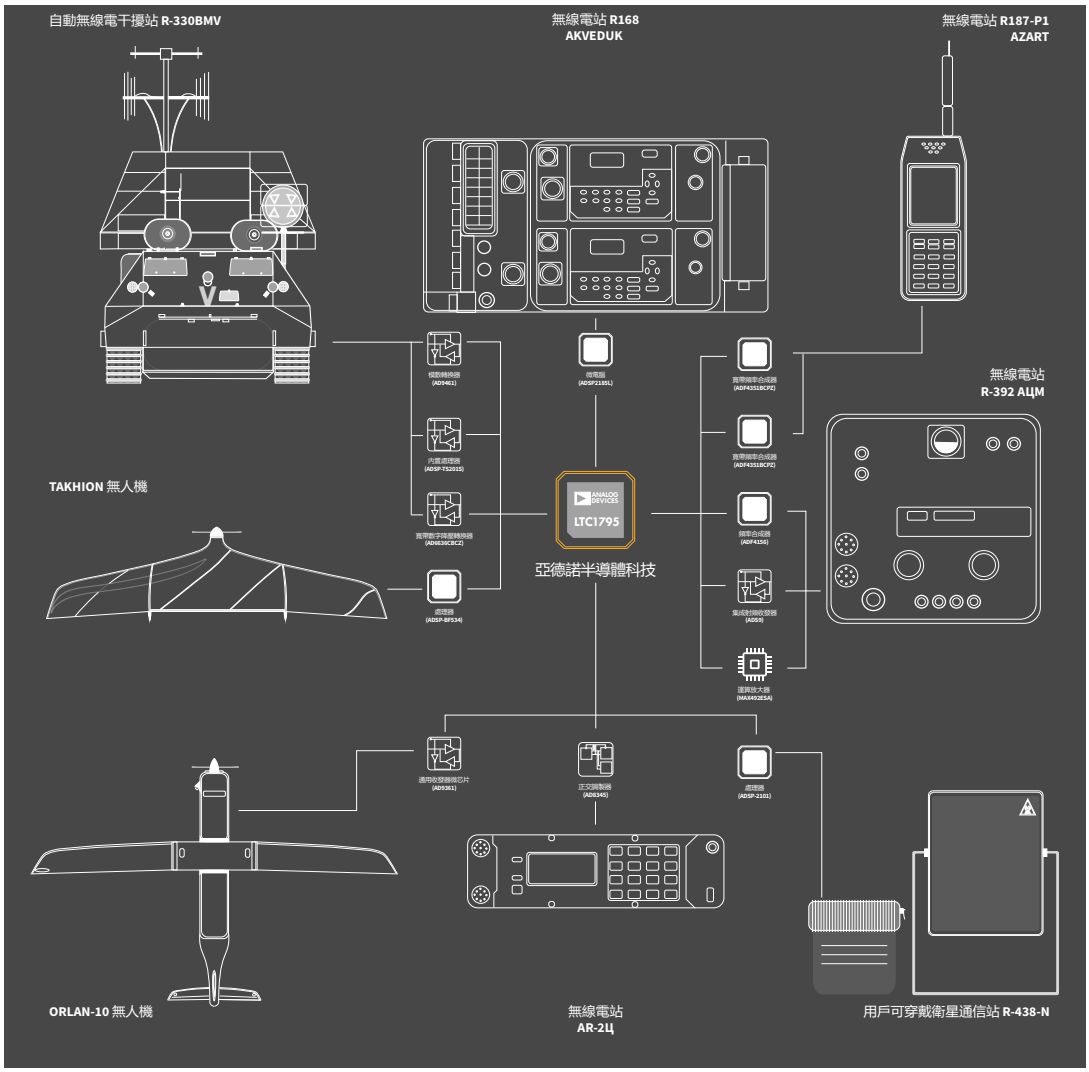
54 ECCN 3A991.a.2 —— 時鐘頻率超過25 MHz的微處理器或微控制器。參閱美國商務部工業和安全局，「商業管制清單：第三類——電子產品」，<https://www.bis.doc.gov/index.php/documents/regulations-docs/442-category-3-electronics-design-development-and-production/file>，訪問日期2022年7月19日。

55 ECCN 5A991.g——移動通信設備。參閱美國商務部工業和安全局，「商務控制清單：第5類——電信和「信息安全」，<https://www.bis.doc.gov/index.php/documents/regulations-docs/2336-ccl5-pt1-3/file>，訪問日期2022年7月19日。

56 ECCN 5A991.b —— 用於單通道或多通道通信的電信傳輸設備和系統。參閱美國商務部工業和安全局，「商務控制清單：第5類——電信和「信息安全」

57 ECCN 3A001.a.5.a.5——一種A/D轉換器，具有16位或更高的分辨率，輸出速率大於每秒 6500萬字。閱美國商務部工業和安全局，「商務控制清單：參閱第3類——電子產品」。

Figure 8: 亞德諾半導體技術公司製造的俄羅斯武器中的ECCN零部件



來源：RUSI.

亞德諾半導體技術有限公司成立於1965年，是世界領先的半導體製造商，專門從事用於數據轉換、信號處理和電源管理的集成電路製造。[58] 其中許多產品專為國防和航空航天應用而設計，並被美國軍方用於精密彈藥、航空電子設備、相控陣系統、軍事通信、電子監視系統和無人機。[59]

例如，該公司的A/D轉換器經常被用於如 MIM-104 Patriot SAM和AIM-120 AMRAAM這樣的美國導彈系統。[60] 這些零部件可將搭載的傳感器收集的模擬、真實世界信號轉換為計算機可處理的數字輸出。[61] 在巡航導彈中，它們可使系統的傳感器實時將數據傳輸到所搭載的計算機上，由計算機負責將爆炸力導航至目標。[62]

58 亞德諾半導體技術有限公司，「公司信息」，<https://www.analog.com/en/about-adi/corporate-information.html>，訪問日期2022年7月19日。

59 亞德諾半導體技術有限公司，「航空航天和國防」，<https://www.analog.com/en/applications/markets/aerospace-and-defense-pavilion-home.html>，訪問日期2022年7月19日。

60 軍用航空電子，「亞德諾半導體科技公司為愛國者導彈供應新型A-D轉換器」，2000年2月1日，<https://www.militaryaerospace.com/communications/article/16706596/analog-devices-to-supply-new-ad-converter-for-patriot-missile>，訪問日期2022年7月19日。

61 Arrow，「模擬-數字（ADC）轉換器類型和基本功能」，2019年2月5日，<https://www.arrow.com/en/research-and-events/articles/analog-to-digital-adc-converter-types-and-basic-functions>，訪問日期2022年7月19日。

62 國際貿易部，「OGEL 和貨物檢查工具」，<https://www.ecochecker.trade.gov.uk/spirefox5live/fox/spire/OGEL_GOODS_CHECKER_LANDING_PAGE/new>，訪問日期2022年7月20日。

亞德諾製造的A/D轉換器的一種—— AD9461在俄羅斯陸軍R-330BMV Borisoglebsk-2電子戰系統的干擾板上被找到。A/D轉換器在這些類型的平台中的作用是讓接收器得以在寬頻帶上運行，從而可識別威脅信號，提高平台性能。[63] 與俄羅斯武器平台中的許多其它零部件一樣，[64]這種特殊轉換器被歸類為兩用物品並被限制出口，說明這些零部件可能是有人代表俄羅斯武裝部隊或情報機構秘密採購的。

在俄羅斯武器系統中還發現了由亞德諾半導體科技原產的其它幾個受管制零部件。其中包括在R-330BMV Borisoglebsk-2 EW系統的同一干擾板上發現的 AD6636CBCZ寬帶（數字）接收器信號處理器、Orlan-10無人機有效載荷信息傳輸模塊中的AD9361射頻捷變收發器和一架Takhion無人機的導航和定位模塊中的Blackfin處理器。

RUSI在俄羅斯武器平台中發現了亞德諾製造的十幾種不同類型的受控零部件，還在其它幾個系統中發現了該公司的另外37個零部件。其中包括Kh-59MK AShM和Torn-MDM SIGINT平台中的零部件。這些是非受控零部件，包括運算放大器、RS-232收發器、電源管理微芯片、射頻開關和溫度傳感器等。

德州一切更美好

在烏克蘭拆解的幾個關鍵的俄羅斯武器系統中，德州儀器製造的產品也占主導地位。德州儀器成立於1930年，迄今已發展成為全球銷量最大的半導體公司之一，[65] 據稱擁有超過41,000項專利。[66]與亞德諾半導體技術公司一樣，總部位於達拉斯的德州儀器公司也為航空航天和國防工業設計高端零部件，並且長期以來一直處於軍用電子領域的前沿。[67]

在美國，該公司的軍用級和高性能零部件已被用於各種軍事系統，包括飛機的飛行控制單元、GPS接收器、雷達系統、聲納系統、電子戰系統、智能彈藥等等。[68] 比如該公司的多核數字信號處理器也很受歡迎，被用於處理一些高性能雷達系統中的任務，[69]如可在夜間通過雲收集圖像的軍用合成孔徑雷達。[70]

在幾個俄羅斯系統中發現了德州儀器製造的50多個獨特零部件，包括在9M727對地攻擊巡航導彈上的各種計算和處理模塊中發現的數字信號處理器，在KUB-BLA「神風敢死隊」無人機的電子雷管中發現的CAN收發器，E95M目標無人機和Orlan-10無人機中發現的電源管理模塊，以及俄羅斯陸軍使用的幾種無線電裝置中的音頻編解碼器和轉換器。

63 Rajesh Uppal，「DARPA的超高速模擬-數字轉換器 (ADC) 可提高雷達、電子戰和通信的性能」，IDST，2017年1月25日，<https://idstch.com/technology/electronics/darpa-s-analog-to-digital-converter-adc-programs-to-improve-performance-of-radar-electronic-warfare-and-communications/>，訪問日期2022年7月20日。

64 ECCN 3A001.a.5.a.5——一種A/D轉換器，具有16位或更高的分辨率，輸出速率大於每秒 6500萬字。閱美國商務部工業和安全局，「商業管制清單：第3類——電子產品」。

65 德州儀器，「德州儀器概覽」，<https://www.ti.com/about-ti/company/ti-at-a-glance.html>，訪問日期2022年7月19日。

66 德州儀器，「德州儀器資料頁」，<https://web.archive.org/web/20160719151815/http://www.ti.com/corp/docs/company/factsheet.shtml>，訪問日期2022年7月19日。

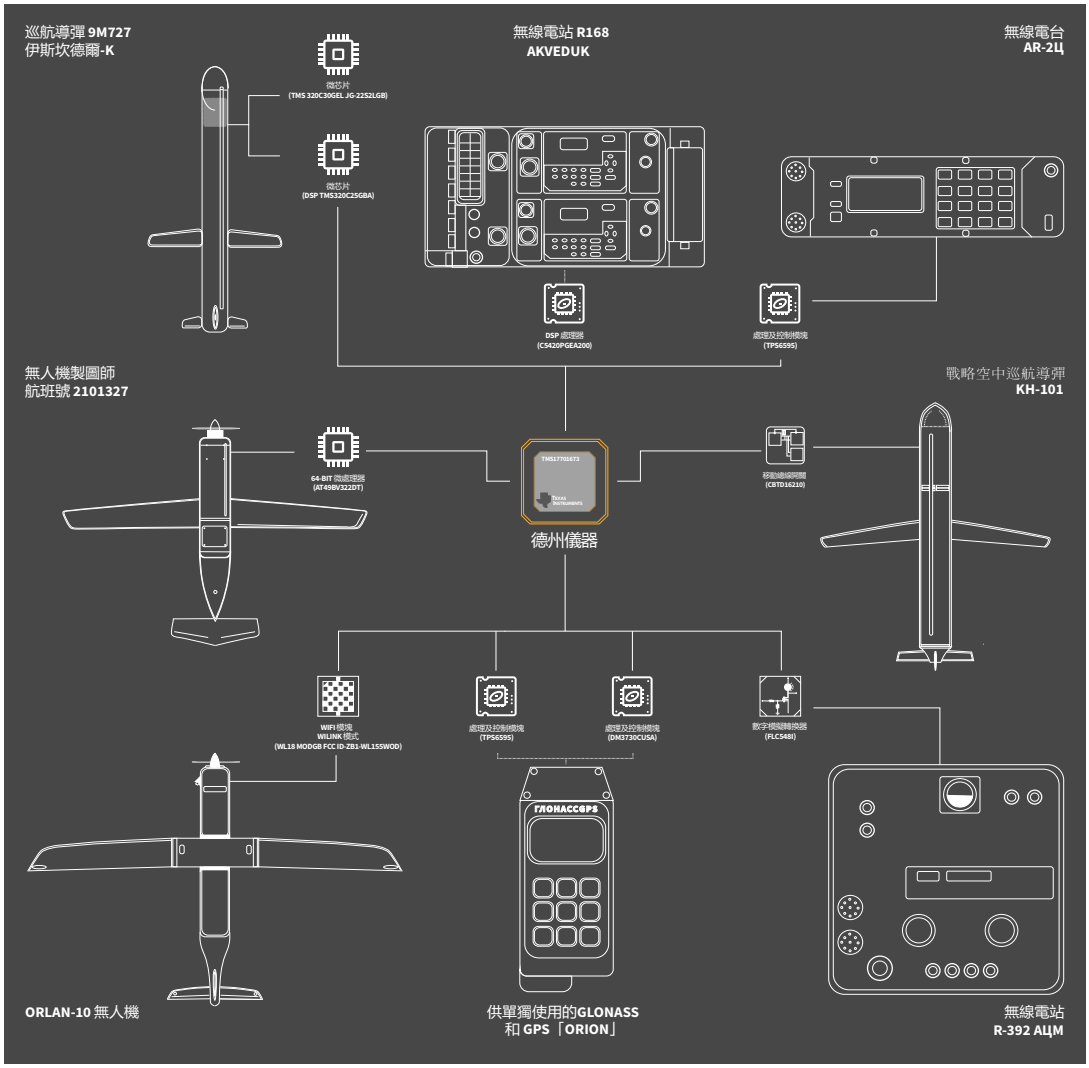
67 德州儀器，「航空航天與國防」，<https://www.ti.com/applications/industrial/aerospace-defense/overview.html>，訪問日期2022年7月19日。

68 Ibid.

69 John McHale，「全新 TI 多核 DSP 支持高性能雷達系統」，軍用嵌入式系統，2012月3月28日，<https://militaryembedded.com/radar-ew/signal-processing/high-performance-radar-systems-enabled-by-new-ti-multicore-dsps>，訪問日期2022年7月20日。

70 Dan Wang及Murtaza Ali，「多核 DSP 增強合成孔徑雷達處理」，軍用嵌入式系統，2013年9月10日，<https://militaryembedded.com/radar-ew/signal-processing/multicore-aperture-radar-processing>，訪問日期2022年7月20日。

Figure 9: 俄羅斯武器中發現的德州儀器製造的ECCN類零部件



來源：RUSI.

在Kh-101 ALCM上還發現了由德州儀器製造的其它零部件， Kh-101 ALCM是一種用於打擊烏克蘭深處目標包括關鍵基礎設施和城市人口中心的精密武器 。[71] 這些零部件有些被安裝在Kh-101的處理器模塊中，該處理模塊是一套幫助引導導彈瞄準目標的系統，例如DS26C32ATM CMOS四差分線接收器，其製造符合軍用標準。[72]

在這些武器平台中發現的由德州儀器製造的零部件中，至少有10個是受美國出口管制的，包括9M727 GLCM中的TMS320 C25GBA和TMS320 C30GEL數字信號處理器。[73]

東京罪惡

雖然美國通常成為俄羅斯非法採購網絡的「頭號目標」，其他擁有先進製造業和半導體行業的國家也位於克里姆林宮的購物清單前列。

在1950年代末和1960年代初，日本戰後的經濟奇蹟將日本推向了全球經濟的前列，這一奇蹟部分歸功於該國蓬勃發展的半導體產業。但隨着索尼和東芝等日本企業集團變得家喻戶曉，它們也引起了克格勃技術間諜團隊的注意。

71 Lorenzo Tondo, 「俄羅斯導彈三週來首次襲擊基輔」, 英國衛報, 2022年6月26日。

72 德州儀器, 「DS26C32ATM/NOPB - CMOS四路差分線路接收器」, <https://www.ti.com/product/DS26C32AT/part-details/DS26C32ATM/NOPB>, 2022年7月20日。

73 ECCN 3A991.a.2 —— 時鐘頻率超過 25 MHz 的微處理器或微控制器。參閱美國商務部工業和安全局, 「商業管制清單：第3類——電子產品」。

1971年6月，日本一家以蘇聯代號TONDA運營的高科技公司的負責人向他的克格勃上司提供了兩卷關於一種新的供美國空軍和導彈部隊使用的微電子計算機系統的秘密文件。[74] 在日本還發生了其它技術情報行動。在1970年代後期，東京居民Oleg Guryanov告訴他的工作人員，「這些［指X線］官員每年執行的行動所獲得的收益支付我們整個東京部門的開支都綽綽有餘。事實上，在世界範圍內，光是技術情報本身就可以支付整個克格勃對外情報部門的所有費用」。[75]

本報告中所分析的武器平台表明，日本技術對俄羅斯武裝部隊仍然很重要。數據集中由日本公司設計和製造獨特零部件共有34個，使其成為美國以外第二大最多見的原產國。這些零部件來自十幾家日本公司，包括松下、佳能等知名公司製造的相機，富士通製造的數字步進衰減器，TDK公司製造的慣性測量單元，以及齋藤製作所製造的航模發動機。

但是，被發現最多的日本零部件還屬日本最古老的電子公司之一村田製作所製造的多層陶瓷電容器和表面貼裝電感器。村田製作所成立於1944年，主要設計和製造基於陶瓷的無源元件和解決方案。[76] 與許多其他電子公司不同的是，村田的網站上懇請其產品不被用於大規模殺傷性武器或常規武器。[77]

然而，俄羅斯人似乎忽視了這一誠懇要求，因為在Torn-MDM SIGINT系統和軍用AR-2C無線電裝置中我們發現了多個村田的零部件。Torn-MDM SIGINT系統是一個相對較新的平台，旨在搜索、分析和記錄無線電信號，同時能確定半徑達70公里內的傳輸方向和位置。[78]

74 Andrew與Mitrokhin，《米特羅欣檔案二》（The Mitrokhin Archive II），第306頁。

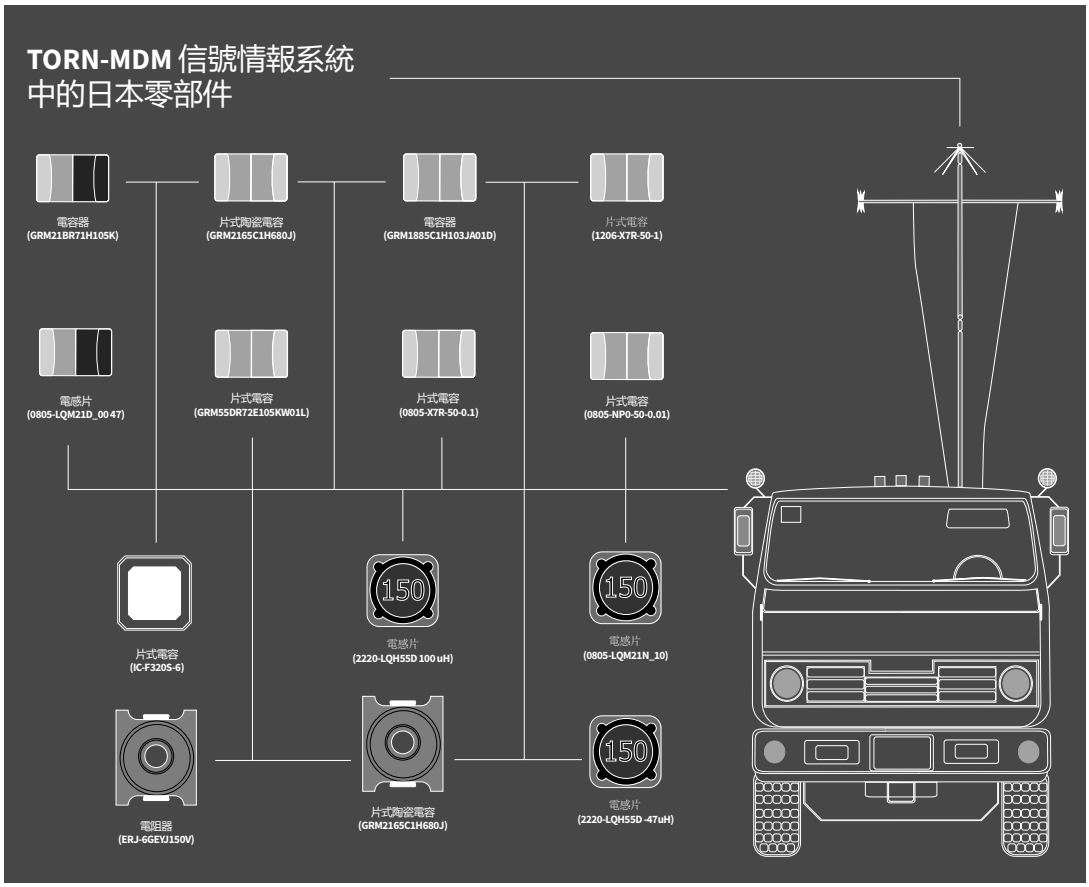
75 Ibid.， 第308頁。最初在Stanilav Levchenko的《錯誤立場：我的克格勃生活》（On the Wrong Side: My Life in the KGB ）（密歇根大學：Pergamon-Brassey 的國際防務出版社：1988)， 第104頁。

76 村田製作所，「事實與數據」，<https://corporate.murata.com/en-global/company/factsandfigures>，訪問日期2022年7月20日。

77 村田製作所，「大規模毀滅性武器和常規武器的限制」，<https://www.murata.com/en-global/support/militaryrestriction>，訪問日期2022年7月20日。

78 烏克蘭軍事中心，「烏克蘭軍隊繳獲了俄羅斯撕裂的 MDM 信號情報系統」，2022年3月17日，<https://mil.in.ua/en/news/ukrainian-army-captured-russian-torn-mdm-sigint-system/>， 訪問日期2022年7月20日。

Figure 10: Torn-MDM SIGINT系統中的日本零部件



來源：RUSI.

各盡所能，各取所需

不僅東亞的半導體產業已成為俄羅斯軍工供應鏈不可或缺的組成部分，西歐國家豐富的科技資產也一直為俄羅斯的特別事務部所垂涎，仍然是俄羅斯技術間諜團隊的優先目標。

這些間諜行動甚至早在1922年12月28日蘇聯成立之前就已經開始了。在1921年或1922年，紅軍總參謀部第四（情報）部（後來更名為GRU）派遣了Aaron和Abraham Ehrenlieb到柏林，在那裡，他們建立了遠東貿易公司，也稱為Wostwag。[79] GRU沿襲了採用商業幌子公司的悠久傳統，將Wostwag用作軍事情報的煙幕，並最終授予該公司對蘇聯武器出口的控制權。[80]

事實證明，在接下來的一個世紀裡，俄羅斯的科技間諜活動和採購活動成了連接兩個通常敵對的政治和經濟體系的紐帶。雖然冷戰的到來引發廣泛禁止向蘇聯出口技術，[81] 冷戰系統在1990年代初期的崩潰卻為克里姆林宮提供了合法購買大量尖端技術的機會，而這些技術都被用在了瞄準烏克蘭和敘利亞的非參戰百姓和民用基礎設施上。

事實上，本報告中所分析的數據表明，歐洲公司製造的零部件在俄羅斯軍事系統中的使用非常普遍。有充分證據顯示法國泰雷茲公司（Thales）製造的凱瑟琳FC熱像儀（Catherine FC）被用在俄羅斯作戰平台上。[82] 然而還不太為人所知的是，俄羅斯採購網絡通常以較小的專業歐洲公司

79 David R Stone, 《1920年代的蘇聯武器出口》（Soviet Arms Exports in the 1920s），當代歷史雜誌（第48卷，No. 1，2013年1月），第57－77頁。

80 Ibid.

81 多邊出口管制協調委員會（CoCom）。

82 Andrew Rettman，「俄羅斯老虎的法國眼睛」，euobserver，2015年8月25日<https://euobserver.com/investigations/129953>，訪問日期2022年7月20日； Oleksandr Dubilet，「法國武器公司衝破制裁，幫助俄羅斯製造武器」，烏克蘭新聲，2022年6月21日。<https://english.nv.ua/business/total-isolation-of-russia/military-thermal-imagers-for-the-russian-army-the-french-company-thales-cooperated-with-russia-aft-50247461.html>，訪問日期2022年7月20日。

為目標，以獲取在其它地方不易採購的高端設備。

鎖定瑞士

俄羅斯武器系統中發現的獨特零部件的第四大製造商是瑞士，數據集中包括了諸如意法半導體和u-blox這樣的瑞士公司，共有18個獨特零部件是由瑞士公司製造的。

意法半導體是一家總部位於日內瓦的法意電子和半導體製造商。[83] 該公司主要製造內存模塊、微處理器、晶體管和微控制器，包括很暢銷的STM32系列。[84] 這些STM32微控制器中有8個是從一系列無人機中找到的，包括 Orlan-10、E95M、Eleron-3SV和KUB-BLA。值得注意的是，這些芯片在這些無人機的幾個子系統中很多見，例如飛行控制器、導航和定位系統以及電源控制板。

鑑於俄羅斯無人機機隊的規模加上在有爭議的空域運行這些平台的高損耗率，俄羅斯武裝部隊必須在2022年2月入侵烏克蘭之前就獲得大量這樣的零部件。然而，這些系統中的好幾個STM32微控制器都受美國出口管制。[85] 意法半導體製造的其它產品有從R-168無線電裝置中的找到的PD55003射頻功率晶體管，和從Kh-101 ALCM的SN-99衛星導航系統中找到的兩個44引腳薄四方扁平封裝。

而u-blox正是支持全球導航衛星系統（GNSS）的半導體和模塊的設計者和供應商，他們設計和製造的產品包括GPS、GLONASS、伽利略、北斗和QZSS的接收器。[86] U-blox的M8系列GNSS模塊出現在Orlan-10的GPS跟踪器、導航和定位系統以及AR-2C無線電裝置中。這些模塊也受美國出口管制。[87]

打通荷蘭

找到的零部件中共有14個來自荷蘭製造商，其中10個來自恩智浦半導體（以下簡稱 NXP），另外兩個來自其前子公司安世半導體（Nexperia）。儘管NXP在總數據集中所佔的數量很少，但卻出現在了被分析的27個系統中的10個中。

被用得最多的是壓力傳感器，例如MPXV5004DP、MPXV5010DP和MPXV5010GP，它們出現在 KUB-BLA、Orlan-10和E95M無人機的飛行控制器中。KUB-BLA的飛行控制器上還安裝了一個NXP製造的微控制器 LPC2368FBD100，該部件為美國管制產品。[88] 其它NXP製造零部件還有在幾個無線電裝置和GLONASS/GPS GROT-M導航設備中發現的射頻晶體管。尤其是在Kh-101 ALCM的BT33處理器模塊中還找到了NXP和安世半導體製造的總線收發器。

攻克倫敦

英國這一擁有廣泛國防工業基礎的發達經濟體，一直成為俄羅斯技術間諜活動的頭號目的地。據悉，克格勃的一大批X線官員曾於1980年代駐紮在倫敦參與間諜活動，他們的主要目標之一是航空航天和國防集團勞斯萊斯。[89]

83 領英，「意法半導體」，<https://www.linkedin.com/company/stmicroelectronics/>，訪問日期2022年7月20日。

84 意法半導體，「主頁」，<https://www.st.com/content/st_com/en.html>，訪問日期2022年7月20日。

85 ECCN 3A991.a.2 —— 時鐘頻率超過25 MHz的微處理器或微控制器。見美國商務部工業和安全局，「商業管制清單：第3類——電子產品」。

86 u-blox,「經久耐用的產品」，<https://www.u-blox.com/en/we-build-last>，訪問日期2022年7月20日。

87 ECCN 7A994 – 導航測向設備、機載通信設備、飛機慣性導航系統和其它航空電子設備。見美國商務部工業和安全局，「商業管制清單：第7類 – 導航與航空電子設備」，<https://www.bis.doc.gov/index.php/documents/regulations-docs/2339-category-7-navigation-and-avionics-2/file>，訪問日期2022年7月20日。

88 ECCN 3A991.a.2 —— 時鐘頻率大於25 MHz的微處理器或微控制器。見美國商務部工業和安全局，「商業管制清單：第3類——電子產品」。

89 國防部長辦公室，「蘇聯獲得具有重要軍事意義的西方技術：更新」，1985年9月，https://apps.dtic.mil/sti/pdfs/ADA160564.pdf>，訪問日期2022年7月21日。

雖然在找到的武器系統中只發現了五個英國製造的零部件，但其中一些零部件相當專業化，例如振盪器和標準晶體。這些特殊零部件由Golledge Electronics設計和製造，該公司專門從事製造電子行業所需的頻率控制產品。[90] 該公司總部位於英格蘭西南部，產品出口到50多個國家。[91] 與上述其他公司一樣，該公司還製造一系列商用現貨產品以滿足多項軍用標準的要求。[92] 2022年3月上旬，該公司宣稱，既俄羅斯入侵烏克蘭後，公司已於2月24日停止在俄羅斯的業務。[93]

Golledge製造的零部件是從如Torn-MDM、Tor-M2 SAM等更複雜的俄羅斯系統中被找到的。前者裝有Golledge製造的HC49標準晶體，而後者的專用數字計算單元裡安裝了一個GXO-U100F振盪器。這兩個零部件通過利用壓電材料製成的振動晶體的機械共振可產生精確頻率的電信號。[94] 這對於Tor-M2等使用雷達探測和跟踪目標的系統至關重要，能提高SIGINT和EW系統的效率。

滲透柏林

俄羅斯運作的間諜網絡包含一系列歐洲國家，德國當然也毫無例外，經常成為俄羅斯採購計劃的核心目標。東德在冷戰時期成為了蘇聯間諜的關鍵目標，被作為獲取西方技術的樞紐。俄羅斯情報部門在東德招募X線特工後，可以很容易地將他們派往聯邦共和國收集信息並滲透到各個重要的德國公司。[95] 1985年，有一項評估聲稱西德在控制對蘇聯的非法出口方面的舉措「無效」，他們只會在美國的壓力下被動採取行動。[96]

90 Golledge Electronics, 「關於我們」, <https://www.golledge.com/about-us/>, 訪問日期2022年7月20日。

91 Ibid.

92 Golledge Electronics, 「用於國防和航空航天的 Mil-COTS 頻率零部件」, 2016年6月28日, <https://www.golledge.com/news/using-mil-cots-for-defence-and-aerospace/>, 訪問日期2022年7月20日。

93 Golledge Electronics, 「Golledge 已退出俄羅斯業務」, 2022年3月11日, <https://www.golledge.com/news/russian-business-withdrawal-aid-for-ukraine/>, 訪問日期2022年7月20日。

94 Sluiceairfair.com, 「壓電振盪器的原理是什麼？」, 2020年8月31日, <https://www.sluiceartfair.com/2020/popular-lifehacks/what-is-the-principle-of-piezoelectric-oscillator/>, 訪問日期2022年7月21日。

95 國防部長辦公室, 「蘇聯獲取具有重要軍事意義的西方技術：更新」。

96 Daniel Salisbury, 「對抗柏林技術隧道：冷戰時期非法武器貿易中的朝鮮特工、直升機和情報, 1981-1986」,
情報與國家安全 (2022).

同年，在代號為出埃及記的行動中，美國當局追查了一個龐大而復雜的蘇聯微電子採購網絡，該行動由海關主導，旨在阻止關鍵技術流向俄羅斯。該網絡由一位名叫Richard Mueller的德國人擔任總指揮，主要任務是「轉移精密的計算機設備」，幫助提高蘇聯的軍用級半導體製造能力。[97] 1980年代中期，美國海關認定Mueller為世界頭號武器走私犯之一。[98]

但其實還有其他高級特工分散活動在德國境內。1984年，在科隆和莫斯科都設有辦事處的伊朗人Babeck Seroush[99] 因向朝鮮出口143種用於導彈制導系統和夜視設備的半導體而被美國法院起訴。[100] 而就此前兩年，同樣被認為是由克格勃招募的 Seroush[101] 被捲入一起涉及將電子元件轉運到蘇聯的案件。[102]

當時，弗拉基米爾・普丁本人和俄羅斯最大的國防集團現任負責人謝爾蓋・切梅佐夫（Sergey Chemezov）都是駐德累斯頓（Dresden）的克格勃官員。[103] 從一張1980年代拍攝的模糊照片可以看到，他們年輕時在德累斯頓時就在一起。[104] 普丁上台後，切梅佐夫追隨其後，2007年，普丁讓他的這位老同事掌舵Rostec（國家先進技術工業產品開發、製造和出口公司的縮寫），切梅佐夫至今仍擔任該職位。[105]

Figure 11: 普丁和切梅佐夫，據稱拍攝於2021年

來源： Kremlin.ru.

97 Ruth Marcus, 『戰爭「企業家」』（‘Entrepreneurs’ of War），華盛頓郵報，1985 年 8 月 10 日。

98 Ibid.

99 Ellan Cates, 「一位西德出口商被指控犯有陰謀……」， UPI, 1984年11月5日, <https://www.upi.com/Archives/1984/11/05/A-West-German-exporter-has-been-charged-with-conspiracy/3117468478800/>, 訪問日期2022年7月20日。

100 Ibid.

101 Salisbury, 「打擊柏林技術隧道」

102 AP News, 「執行官被控密謀向蘇聯運送電腦板」, 1985年4月25日。

103 經濟學人, 「新克格勃國家的形成」, 2007年8月23日。

104 Rob Lee (@RALee85), 「謝爾蓋・切梅佐夫和弗拉基米爾・普丁1980 年代和今天在德累斯頓」, 推特, 2021年7月20日。<https://twitter.com/ralee85/status/1417560713862828035?lang=en>, 訪問日期2022年7月20日。

105 Rostec, 「謝爾蓋・切梅佐夫向俄羅斯總統匯報 Rostec 2021年的業績」, 2022年7月20日。<https://rostec.ru/en/news/sergey-chemezov-reports-to-president-of-russia-on-rostec-2021-performance-/>, 訪問日期2022年7月20日。

近年來，德國仍然是那些為獲得尖端技術科技而從事間諜活動和搭建採購網絡的目的地。2021年5月，一名德國公民因向俄羅斯情報部門運營的一家公司運送兩用物品而被逮捕。[106] 時隔僅一個月，德國當局又逮捕了一名從奧格斯堡研究中心竊取航空機密和導彈技術的俄羅斯科學家。[107]

RUSI在7個武器系統中發現了10個由德國公司製造的零部件。其中最多見的是由EPCOS AG製造，在Torn-MDM SIGINT系統的多個子系統中發現的濾波器和表面貼裝電感器。EPCOS AG最初由德國西門子和日本松下的合資企業西門子鬆下有限公司（Siemens Matsushita Components）於1999年創立。[108] EPCOS AG後來於2009年被日本TDK株式会社（TDK Corporation）收購，並更名為TDK电子股份有限公司（TDK Electronics AG）。[109] 公司產品目錄包括電容器、陶瓷元件、EMC 濾波器、電感器、射頻模塊等產品。[110]

與此同時，在Eleron-3SV和KUB-BLA無人機上分別找到了Graupner GmbH和Aero Naut製造的气刃。然而，在一套俄羅斯武器系統裡發現了一個美國出口管制物品。這是在R-330BMV EW系統[111]的一個特殊計算機模塊中找到的由Würth Elektronik GmbH製造的局域網變壓器 。

106 AP News，「德國以向俄羅斯出口軍民兩用產品的罪名逮捕商人」，2021年5月18日。

107 Matthias von Hein，「俄羅斯科學家因從事間諜活動在德國受審」，DW，2022年2月17日。

108 Gerhard Fasol，「TDK收購無源電子元件製造商 EPCOS」，Europe-Japan，2008年7月31日，<https://eu-japan.com/2008/07/tdk-epcos/>，訪問日期2022年7月20日。

109 Interference Technology，「EPCOS AG 更名為 TDK Electronics AG」，2018年10月5日，<https://interferencetechnology.com/epcos-ag-changes-its-name-to-tdk-electronics-ag%E2%80%AF/>，訪問日期2022年7月20日。

110 TDK Corporation，「收購 EPCOS AG – 成為電子元件行業的全球領導者」，2009，<https://www.tdk.com/ir/ir_library/annual/web/lib20405.pdf>，訪問日期2022年7月20日。

111 ECCN 3A991.b.2.a – 一種微波單片集成線路功率放大器，預定工作頻率2.7Ghz以上，最高達6.8GHz，分率大於15%。見美國商務部工業和安全局，「商業管制清單：第3類——電子產品」。

第 2 部分

俄羅斯導彈的剖析

2021年12月6日，俄羅斯國有國防承包商金剛石-安泰（Almaz-Antey）的總經理Yan Novikov稱：「在不久的將來，軍事衝突中的戰鬥行動將是一種先進技術之間的較量，而最關鍵的技術是航空航天攻擊武器以及空中和導彈防禦系統。」[112]

在俄羅斯入侵烏克蘭的戰爭打響後的幾個小時裡，俄羅斯武裝部隊向一系列設施發射巡航導彈和彈道導彈，旨在破壞和瓦解烏克蘭的防空和C4ISR[113]系統。[114] 後來，目標被擴大到軍事基礎設施（如容納外國戰士的營房），以及破壞西方供應線的鐵路基礎設施，还包括燃料庫、武器工廠，甚至醫院和購物中心等民用目標。

俄羅斯武裝部隊擁有大量此類武器，據悉，截至5 月初，他們已消耗了 2,000多枚導彈。[115] 這些武器包括俄羅斯空軍使用的Kh-101 ALCM，被用來從俄羅斯安全領空打擊目標，[116]而俄羅斯陸军则部署了通常從俄羅斯領土發射的 9M720和9M727伊斯坎德爾彈道導彈和巡航導彈。[117]

儘管這些系統在擊中目標過程中有很多都被摧毀，但其中一些已被恢復並被拆解，使得我們能夠對其構造進行詳盡的分析。

112 Yan Novikov，金剛石-安泰公司總經理：「空中和太空能力将在未来的衝突中起决定性作用」，DefenseNews，2021年12月6日 。

113 指揮、控制、通信、計算機（C4）情報、監視和偵察（ISR）

114 Justin Bronk，「俄羅斯空軍失踪之謎」，RUSI Commentary，2022年2月28日。

115 美國國防部，「高級國防官員舉行背景簡報會」，記錄文本，2022年5月2日。<https://www.defense.gov/News/Transcripts/Transcript/Article/3017053/senior-defense-official-holds-a-background-briefing/>，訪問日期2022年7月20日。

116 NBC News，「俄羅斯導彈數週以來首次襲擊基輔，據報造成2人死亡」， 2022年6月22日。

117 Kyiv Independent，「總參謀部：俄羅斯在別爾哥羅德州部署伊斯坎德爾導彈發射器」，2022年5月22日。

02

這些武器是由一系列子系統集成的，參與生產其中的零部件的製造商的網絡極其複雜。儘管這些網絡可能觸角廣泛，但通常可以被追溯到相同的源頭：俄羅斯的兩個主要國有國防企業集團Rostec和金剛石-安泰（OAO Concern VKO「Almaz-Antey」，即金剛石-安泰科研生產聯合體康采恩）都因其在供應俄羅斯武裝部隊方面的核心作用，而成為西方國家的目標。

俄羅斯國家技術集團Rostec成立於2007年，至今一直由普丁的知己切梅佐夫領導。[118] 而金剛石-安泰於2002年根據總統令成立，由Yan Novikov主管。但在2014年至2016年期間，該公司的董事會也由切梅佐夫領導。[119]

這些組織龐大，指揮着一系列研究機構、設計局、製造廠和公司，數目之多令人眼花繚亂，它們共同承擔著俄羅斯導彈和其它軍事系統的設計、開發和製造的任務。

伊斯坎德爾9M727

9M727是一種俄羅斯中程地面發射巡航導彈（GLCM），可以在低空飛行以躲避雷達並降低攔截風險。[120] 為了能導航到正確目標並在飛行中修正航向，導彈裝有許多傳感器，以及能將外部信號轉換為數字輸入的內部計算機系統。

Figure 12: 9M727巡航導彈的圖像

來源：RUSI.

118 路透社，「普丁盟友切梅佐夫稱俄羅斯將成為勝利者」，2022年3月10日。

119 Almaz-Antey，「公司歷史」，<http://www.almaz-antey.ru/en/istoriya/>，訪問日期2022年7月21日。

120 CSIS Missile Defense Project（CSIS導彈防禦項目），‘9M729 (SSC-8)’，最後更新於2022年3月31日，<https://missilethreat.csis.org/missile/ssc-8-novator-9m729/>，訪問時間2022年7月21日。

導彈最重要的兩個信號處理系統是Zarya和Baget-62-04計算機，它們分別處理雷達和電視制導（TGM）數據。導彈最重要的傳感器之一是安裝在機身上的一個系統，它能處理GPS和GLONASS 信號——SN-99（C H-99）。

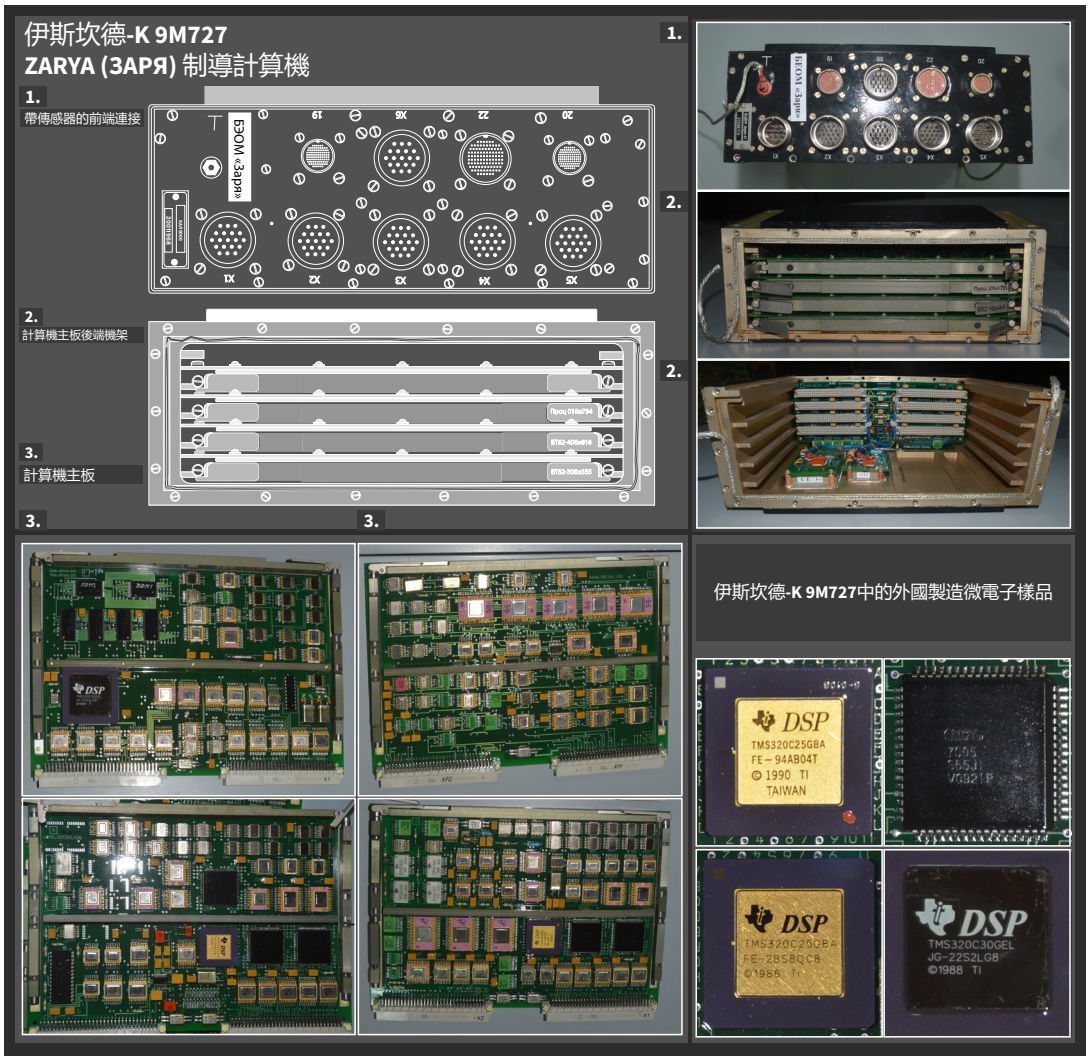
對這些系統的組成部分進行研究後發現它們的結構中有大量的西方製造的零部件，而這些零部件的俄羅斯製造鏈的源頭通常都是Rostec和金剛石-安泰。

ZARYA雷達處理計算機

Zarya計算機被安裝在9M727導彈前端的一個全金屬底盤內，通過一個金屬定位塊將其固定。如此堅固的結構是為了保護計算機免受振動和衝擊的影響，避免在導彈發射和到達目標過程中操作收到干擾。金屬底盤還能保護計算機免受電磁干擾，同樣，用一個編織金屬墊圈將安裝在9M727機身內的計算機密封也是出於這個原因。

這樣，Zarya就能被動冷卻，即不需要風扇或通風口來控制溫度。這為電子裝置提供了一定的抗水損害能力以及抗振動能力，如果系統依賴主動式冷卻機制，則可能干擾系統操作。

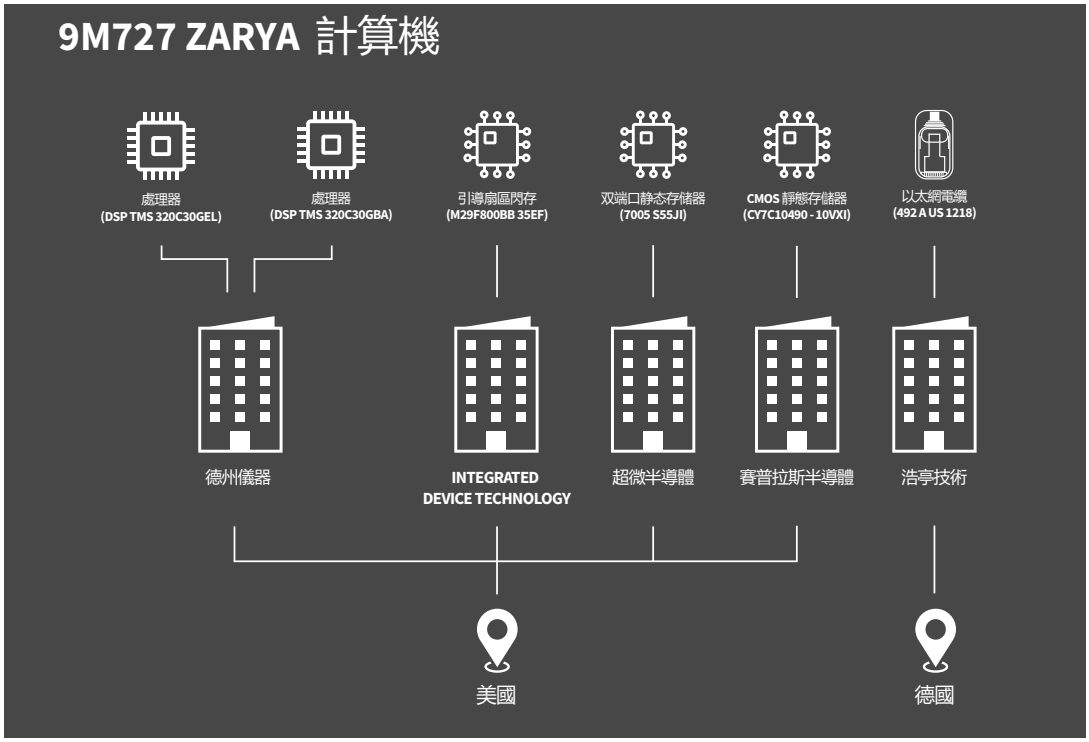
Figure 13: Zarya計算機的拆解



來源：RUSI.

至少某些型號的Zarya計算機製造商歷來都與俄羅斯軍用系統製造實體相關，即最終與金剛石-安泰相關。[121]然而，從9M727上發現的Zarya計算機中還是找到了幾個來自西方的零部件，包括來自美國和德國公司的數字信號處理器、閃存模塊、靜態RAM模塊和以太網電纜。

Figure 14: Zarya計算機中的西方零部件



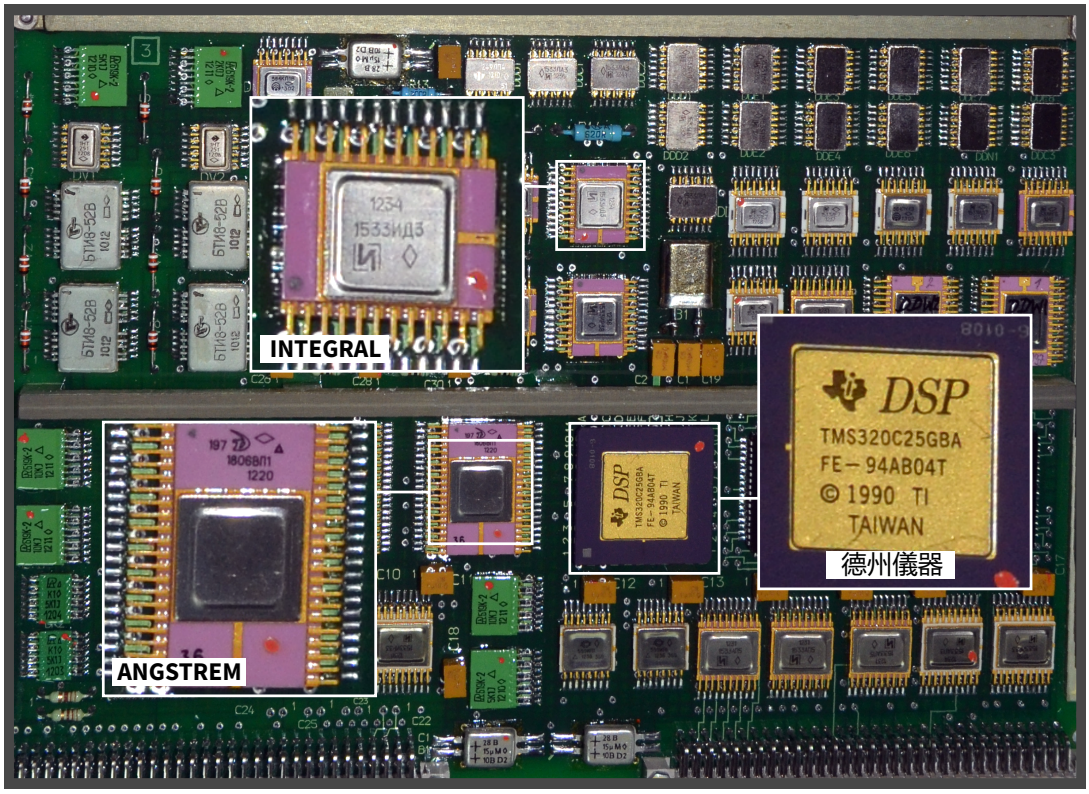
來源：RUSI.

121 一份署名莫斯科航空學院的A.N. Shishkov的文件指出，在 1990 年代初期，莫斯科的「NII Priborostroeniya」製造了一系列Zarya模型。A H Shishkov，「Lekcija Mikroprocessory [微處理器講座]」，莫斯科航空學院，p。 38，<http://frela-mk.narod.ru/olderfiles/1/Lekcciya_3_4_Mikroproccessory.pdf>， 訪問日期2022年7月28日。這可能是指 V.V.Tikhomirov 儀器設計科學研究所（NIIP）或國家儀器設計研究所（Gosniip）。這兩個實體都參與了軍事技術的製造。見 V.V.Tikhomirov 儀器設計科學研究所，[「出口製造」]，<https://www.niip.ru/catalog/eksportnaya-produktsiya>，訪問日期2022年7月26日；Army Recognition,「俄羅斯擁有比預期更多的SSC-8巡航導彈，射程帶衝突性質」，2019年2月11日，<https://www.armyrecognition.com/february_2019_global_defense_security_army_news_industry/russia_has_more_ssc-8_cruise_missiles_than_expected_with_conflictual_range.html>，2022年7月28日；俄羅斯戰略核力量，「巡航導彈和 INF - 9M729 呢？」，2015年6月23日，<https://webcache.googleusercontent.com/search?q=cache:kGNi1MZkOSIJ:https://russianforces.org/blog/2015/06/cruise_missiles_and_inf_-_what.shtml+&cd=2&hl=en&ct=clnk&gl=de>，訪問日期 2022 年 7 月 28 日。在撰寫本文時，NIIP 的控股方為金剛石-安泰和Rostec 。見Oruzhiye Rossii 的[俄羅斯武器]，‘Nauchno-izsledovatel’skij institut priborostroenniya imeni V.V.Tikhomirova, AO [V.V.Tikhomirov 儀器設計科學研究所, JSC]，<https://www.arms-expo.ru/armament/ members/625/83161/>，訪問日期 2022 年 7 月 21日。GosNIIP 早在 2018 年就是金剛石-安泰的一部分，並且GosNIIP網頁上仍然突出顯示金剛石-安泰的公司徽標。見GosNIIP，[股份公司「國家儀器儀表設計研究院」]，<http://www.gosniip.ru/>，2022年7月28日；弗拉基米爾・梅德韋傑夫，「Frontovyje aviacionnye pribory i ih sozdateli」[前線航空儀器及其創造者]，Nacional’naya oborona [National Defence]，2018年2月27日，<https://2009-2020.oborona.ru/includes/periodics/defense/2018/0227/122323529/print.shtml>，訪問日期2022年7月28日。

值得注意的是，Zarya系統的核心處理器似乎是德州儀器製造的數字信號處理器。這些處理器用於以重複方式處理數據流，並可以對導彈機載傳感器收集的數據進行過濾、處理和轉換。

Zarya的數字信號處理芯片是德州儀器的TMS320系列，最初於1983年發布，但此後經過多次改良。RUSI檢查的9M727電路板既有C25也有C30，後者每秒可進行高達5000萬次操作，這在當初製造時可能是市場上能找到的最高版本。微芯片的日期在1988年和1990年間，表明該系統可能是在1980年代末至1990年代初設計和製造的。數字信號處理器似乎還與Integrated Device Technology或賽普拉斯半導體公司製造的其它來自西方的內存芯片相配合使用。

Figure 15: Zarya電路板上的Angstrem和Integral微芯片



來源：RUSI.

通過Angstrem和Integral製造的國產芯片上的徽標便能判斷出，系統中看到的金屬封裝集成電路器件主要是蘇聯產的。在蘇聯解體之前，Angstrem和Integral以及總部位於莫斯科的PAO Mikron[122]是該國集成電路的主要製造實體。在列寧格勒精密機械科學研究所的支持下，Angstrem成立於1963年，，並開發了第一款國產Tropa系列微芯片。[123] 此後，該公司製造了超過2,000種微芯片和半導體器件，用於導彈制導系統、空間和航空技術、個人計算機和微型計算器等應用。[124]

122 Mikron的歷史可以追溯到1950年代後期，最初為Voronezh半導體器件工廠 (Voronezhskij zavod poluprovodnikovyh priborov)，該工廠後來成為VZPP-Mikron。Mikron歷來製造用於軍事系統的零部件。見Mikron, 「Mikron 歷史」, <https://en.mikron.ru/company/history/>, 訪問日期2022年6月30日。

123 Angstrem, 「Katalog produkcii」【產品目錄】, 2022年, <https://tinyurl.com/6mcp38rp>, 訪問日期2022年7月21日。

124 Ibid.

2018年，Angstrem超過 91%的總銷售額來自軍用產品； 而國內市場銷售的數字則超過96%。[125] Angstrem是AO Angstrem-T的大股東，其資產於2022年2月22日被「外國資產控制辦公室」(OFAC) 凍結。[126]

而Integral是一家位於白俄羅斯的製造商，專門從事集成系統、分立半導體器件和信息顯示系統製造，包括（根據該公司的網頁介紹）集成到極端條件下部署的專用設備中。[127] Integral於1960年代開始製造，但因俄羅斯入侵烏克蘭而於2022年2月24日受到OFAC的制裁。[128]

BAGET計算機

在伊斯坎德爾-K 9M727中發現的另一台計算機是Baget-62-04——一種主要用於在最終階段確保精確定位的電視制導處理系統。俄羅斯科學院系統分析科學研究所 (SRISA RAS) 的一名研究人員在最近的一篇文章中將Baget系列計算機描述為用於信號處理的高性能設備。[129]

與Zarya計算機一樣，Baget-62-04的電子設備被封裝在一個專門的系統中，確保其免受高破壞性負載因素和電磁干擾的影響。Baget-62-04上還安裝有一系列西方製造的零部件，包括微處理器、FPGA、SRAM芯片、晶體振盪器、連接插座和一系列其它零部件。

125 Angstrem,「Angstrem 股份公司2018年年度報告」, 經公司總經理兼總會計師於2019年6月28日確認的報告 ，第7頁。在Interfax, 訪問，Centr Raskrytiya Korporativnoj Informacii 「企業信息查找中心」, <https://www.e-disclosure.ru/portal/files.aspx?id=3782&type=2&attempt=1> , 訪問日期2022年7月1日。

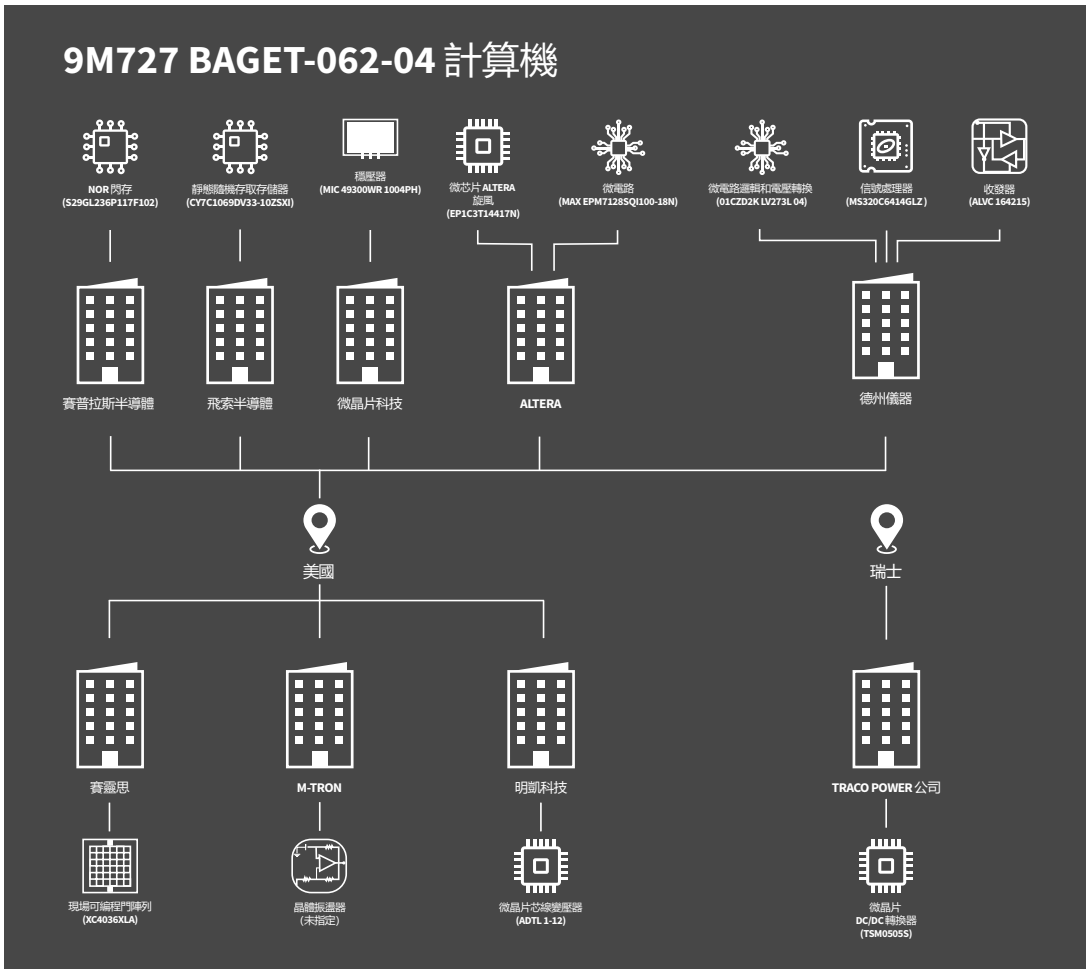
126 美國財政部, 「美國財政部對頓涅茨克和盧甘斯克地區的行動施加直接經濟成本」, 新聞稿, 2022年2月22日, <https://home.treasury.gov/news/press-releases/jy0602>, 訪問日期2022年7月21日。

127 Integral, 「Produkciya」（產品）, <https://integral.by/ru/products>, 訪問日期2022年7月20日。

128 美國財政部, 「美國財政部對頓涅茨克和盧甘斯克地區的行動施加直接經濟成本」

129 Antonov A A 及 A A Krasnyuk, 「工業控制和數據處理系統微處理器的內部結構」, IOP會議系列: 材料科學與工程（2021年第1061號）。 .

Figure 16: Baget-62-04中的西方零部件



來源：RUSI.

Baget系列的歷史可以追溯到蘇聯解體後，當時，俄羅斯政府為減少對外國供應商的依賴，努力在國內製造軍用計算機和零部件。[130] 俄羅斯製造商出版的一份2017年的宣傳冊顯示，一種可能是Baget 64-02下一代產品將作為機載控制系統用於航空綜合設施以及地面和空中高精度武器綜合設施中。[131]

該宣傳冊由AO設計局「Korund-M」（KB Korund-M）和俄羅斯的SRISA RAS合著，宣傳了一系列Baget計算機和為軍事應用而設計的國產微芯片。

130 AO Konstruktorskoe b'uro (KB) Korund-M (JSC 設計局 (DB) Korund-M) 和「俄羅斯科學院系統分析研究所 (FSI FSC SRISA RAS)」,「Baget 家族的未來計算機」，2017年，第2-3頁。

131 Ibid.

Figure 17: KB Korund-M和SRISA RAS宣傳的現代Baget計算機系統

來源：Korund-M和SRISA RAS宣傳冊。

[132] 似乎隸屬SRISA RAS設計局的KB Korund-M在其網頁上指出，其產品已被部署在俄羅斯軍事系統中，包括伊斯坎德爾導彈綜合體，並且他們還在繼續製造具有軍事用途的計算機，並進行與俄羅斯國防部計算需求相關的研發。[133] SRISA RAS於2022年8月2日被OFAC制裁。[134]KB Korund-M沒有被西方政府制裁。[135]

Baget-62-04在AO Serpukhov Metallist Plant的年度報告中也被提到，聲稱該公司在2013年為伊斯坎特爾-M 導彈製造了222台Baget-62-04計算機，計劃製造269台Baget-62-03計算機。[136] 2021年[137]发布的2020年的工廠年度报告中，仍然提到参与Baget计算机生产的情况。2022年6月發布的2021年年度報告沒有提及Baget計算機。[138]

132 Vladimir Betelin是該公司的創始人之一，也是SRISA RAS的科學主任。見俄罗斯科学院系统分析联邦政府机构科学研究所「Betelin Vladimir Borisovich」，<https://www.niisi.ru/betelin.htm>，訪問日期2022年7月25日。在2020年7月24日的俄羅斯聯邦稅務文件中，Betelin被列為AO KB Korund-M的總經理和主要股東。 2021年12月4日的俄羅斯聯邦稅務文件還將Betelin列為自治非商業組織設計局 Korund-M的主管，而SRISA RAS被列為該公司的股東。2022年6月16日的俄羅斯聯邦稅務文件仍將Betelin列為公司董事，但未提及SRISA RAS。可以通過Sayari Labs查閱俄羅斯聯邦稅務登記處文件，<https://sayari.com/>，訪問日期2022年7月22日。

133 Konstruktorskoye B’uro Korund-M［設計局 Korund-M］，‘O “Korund-M”’ ［關於 Korund-M ］，<https://kbkorund.ru/about>，訪問日期2022年7月26日。

134 美國國務院，「就俄羅斯對烏克蘭的戰爭的持續而施加額外成本」，情況說明書，2022年8月2日，<https://www.state.gov/imposing-additional-costs-on-russia-for-its -continued-war-against-ukraine/>，訪問日期2022年8月2日。

135 Baget的某些型號——即 Baget-53計算機——看來也由Ramenskoye儀器製造設計局製造。見開放股份公司，「OJSC 電子產品目錄 Ramenskoye 儀器製造設計局」，2013年，第14頁，<https://mniirip.ru/sites/default/files/articles/katalog_elektronnogo_napravleniya_rpkb.pdf>，訪問日期2022年7月20日。

136 「開放股份公司 Serpukhov Plant Metallist 2013 年度年報」，2014年，第16頁。訪問Interfax， JSC Serpukhov Plant Metallist，「企業資訊查找中心」，<https://www.e-disclosure.ru/portal/files.aspx?id=23097&type=2>，訪問日期2022年7月1日。

137 見，如，「開放股份公司 Serpukhov Plant Metallist 2020 年度年報」，2021年，第16頁。訪問Interfax，JSC Serpukhov Plant ‘Metallist，「企業資訊查找中心」，<https://www.e-disclosure.ru/portal/files.aspx?id=23097&type=2>，訪問日期2022年7月1日。

138 「開放式股份公司年報 Serpukhov Plant Metallist2021年度年报 」。訪問 Interfax，「AO Serpukhovskij Zavod Metallist」’，「企業資訊查找中心」，<https://www.e-disclosure.ru/portal/files.aspx?id=23097&type=2>，訪問日期2022年7月28日。

Serpukhov Metallist工廠由蘇聯聯邦國防委員會於1943年11月建立，設施龐大，歷來參與蘇聯和俄羅斯軍事技術的製造，據報導直到最近還在繼續關鍵軍事零部件的製造活動。[139] [140] 截至2021年12月，該工廠歸Rostec的JSC NPO高精度系統公司（AO NPO Vysokotochnye Kompleksy）所有。 [141]

NPO 高精度系統公司是一家俄羅斯國有控股公司，於2022年3月受到美國財政部的製裁。據美國財政部稱，在2022年2月俄羅斯入侵之前，NPO高精度系統公司製造的一些導彈系統（包括伊斯坎德爾）被運到了俄羅斯-烏克蘭邊境。[142]

導航系統

近二十年來，俄羅斯的軍事理論一直依賴於使用遠程和中程巡航導彈來打擊對手領土深處的關鍵軍事基礎設施。為了確保這些武器擊中目標，俄羅斯武裝部隊開發了先進的慣性和導航傳感器，可以在低空操作時引導導彈以避開防空系統。在9M727和Kh-101空射巡航導彈上發現的關鍵傳感器之一是GLONASS和GPS 制導單元SN-99（C H-99）。

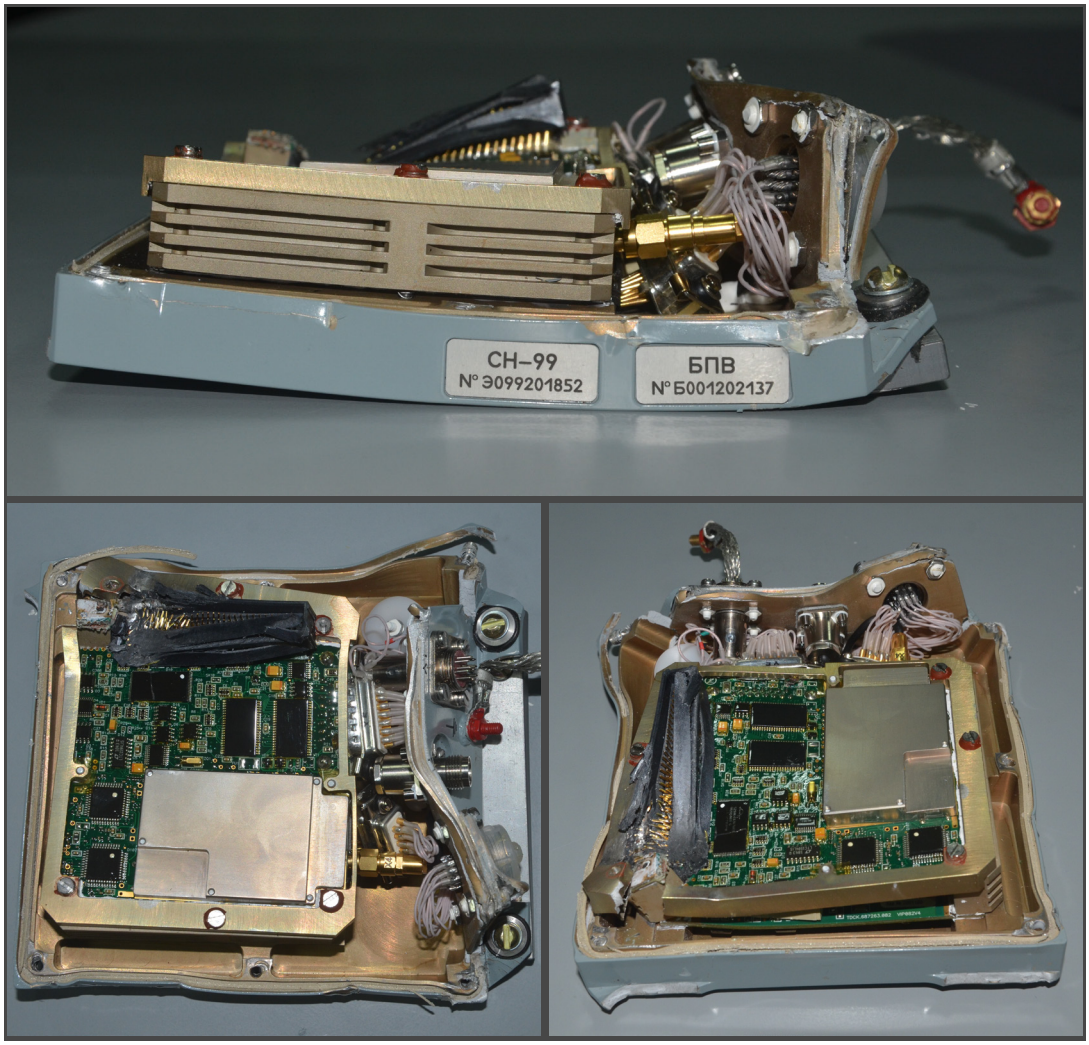
139 Oleg Falichev, Metallist: 目標部門, Military-Industrial Courier, 2018年11月6日, <https://vpk-news.ru/articles/46107>, 訪問日期2022年7月21日。

140 Serpukhovskie Vesti，「Serpuhovskomu zavodu Metallist ispolnyaetsya 75 let」（Serpukhov Metallist工廠成立75週年），2018年8月13日，<http://inserpuhov.ru/novosti/proizvodstvo/serpuhovskomu-zavodu-metallist-ispolnyaetsya-75-let>, 訪問日期2022年7月20日。

141 Serpukhov Plant Metallist, [主頁], 2021年12月26日獲得的網頁存檔版本, <https://web.archive.org/web/20211226064918/http://www.szmetallist.ru/>, 訪問日期 2022年7月21日。

142 美國財政部，「U.S. 財政部製裁俄羅斯國防工業基地、俄羅斯杜馬及其成員以及Sberbank首席執行官」，新聞稿，2022年3月24日，<https://home.treasury.gov/news/press-releases/jy0677>, 訪問日期2022年7月21日。

Figure 18: SN-99 (C H-99) GLONASS和GPS制導系統的圖像



來源：RUSI.

該裝置由俄羅斯軍方使用的GLONASS、GPS和伽利略導航系統製造商導航系統設計局（AO KB NAVIS）[143]製造。[144] 俄語公司記錄[145]和期刊還聲稱，上述SRISA RAS設計局KB Korund-M創立了KB NAVIS。[146]與KB Korund-M一樣，KB NAVIS並未受到西方政府的制裁，儘管它為俄羅斯導彈計劃提供了關鍵技術。

143 Konstruktorskoye B’uro Navigacionnyh Sistem Navis 【導航系統設計局Navis】，「SN-99 Navigacionnaya apparatura dlya vysokodinamichnyh ob’ektov GLONASS/GPS/SBAS」【SN-99 – 用於GLONASS/GPS/SBAS高動態對象的導航設備】，<https://navis.ru/assets/files/SN-99---korrekt_NEW.pdf>，訪問日期2022年7月21日。

144 「Nekommercheskaya organizaciya Associaciya razrabotchikov, proizvoditelei i potrebitelei oborudovaniya i prilozhenij na osnove global’nyh navigacionnyh sputnikovyh sistem GLONASS/GNSS-Forum」【以全球衛星導航系統GLONASS/GNSS-Forum為基礎的設備和應用開發者、製造者和消費者協會的非商業組織】，「Analiticheskij otchet po itogam izsledovaniya sostoianiya i perspektiv razvitiya rynka navigacionnyh, svyazanyh i navigacionno-sviazannyh modulej, a takzhe ocenki vliyanniya na razvitie rossijskogo i mezhdunarodnogo rynka “Avtonet”」【關於導航、網絡和導航網絡模塊市場狀況和發展前景的研究結果的分析報告，以及對俄羅斯和國際「Autonet」市場發展的影響評估】，2019，<https://tinyurl.com/yckfrxwx>，第189頁，訪問日期2022年7月15日。

145 參閱俄羅斯聯邦稅務登記處，2020年7月9日文件，摘自 Sayari Labs，<https://sayari.com/>，訪問日期2022年7月10日。

146 A A Shanin et al.，「Apparatura Sputnikovyh Navigacionnyh Sistem GLONASS i GPS Konstruktorskogo B’uro Navigacionnyh Sistem」【衛星導航系統設備導航系統設計局的GLONASS和GPS】，導航和水文，國家研

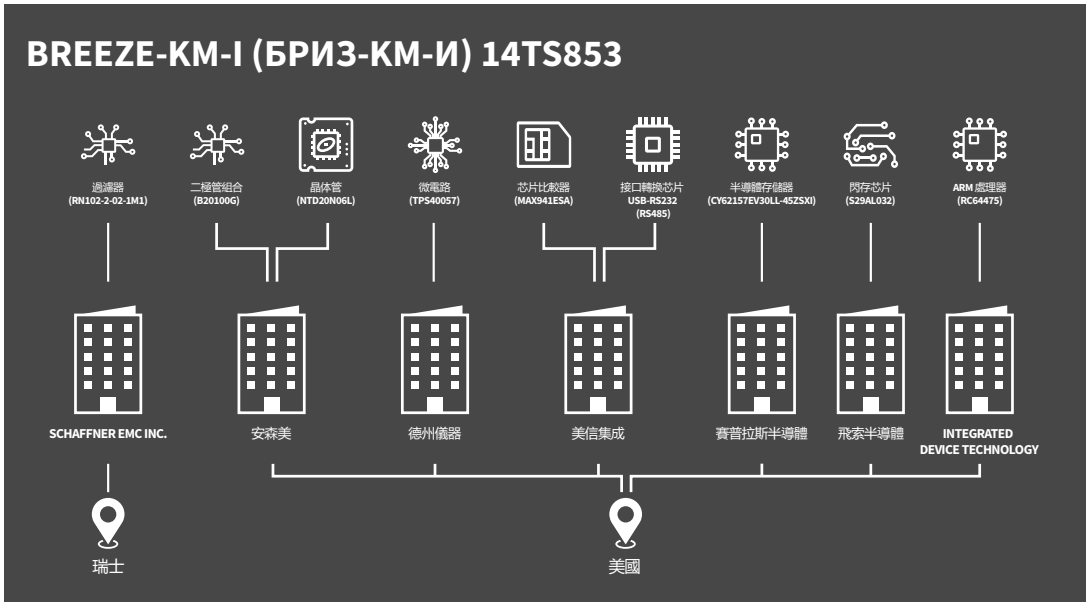
值得注意的是，SN-99（ＣＨ-99）系統包含幾個西方製造的零部件，例如由Spansion製造的32兆位閃存芯片和由凌力爾特公司製造的12位A/D轉換器。儘管按現代標準，12位範圍內的A/D轉換器不再被認為不尋常，但它仍然是戰術巡航和彈道導彈的關鍵部件，並且在SN-99系統組裝的當時可能被認為是頂級的。

多種產品

然而，KB NAVIS 似乎為俄羅斯軍方製造了數件設備。其中就還有俄羅斯特種作戰部隊（SOF）使用的名為 Breeze-KM-I[147]的手持導航和定位系統。特種作戰部隊和前沿偵察人員通常使用這些類型的設備來準確定位己方位置並對精確火砲和空襲敵方位置的坐標作出估計。

拆解後發現Breeze-KM-I中安裝了許多西方製造的微電子元件，包括高性能64位微處理器、SRAM芯片、收發器和放大器。

Figure 19: Breeze-KM-I中的零部件



來源：RUSI.

其中一個零部件是最初由美國賽普拉斯半導體公司製造的高性能CMOS靜態RAM芯片(CY62157EV30LL-45ZSXI)。這是一種高速、超低功耗的存儲芯片[148]， 屬於出口兩用商品。[149]

根據俄羅斯貿易記錄和進口報關單，2017年至2021年間，KB NAVIS進口了由亞德諾半導體科技公司、德州儀器公司和凌特公司（Linear Technology）等美國公司製造的大量電子產品、集成電路和其它電子元件。[150] 儘管大部分貨物是美國製造的商品，但其中絕大多數是通過瑞士、以色列、中國和馬來西亞運來的。[151]

究導航水文研究所，俄羅斯聯邦國防部，2001年12月，第173頁。

147 NAVIS，「Breeze-KM-I個人導航GLONASS/GPS/SBAS 設備」，<https://navis.ru>，訪問日期2022年6月23日。

148 英飛凌科技，「CY62157EV30 MoBL 8-Mbit (512K × 16) 靜態 RAM」，數據表，2020年2月28 日，<https://www.infineon.com/dgdl/Infineon-CY62157EV30_MoBL_8-Mbit_(512_K_16)_Static_RAM-DataSheet-v20_00-EN.pdf?fileId=8ac78c8c7d0d8da4017d0ebe669131ef>，訪問日期2022年7月21日。

149 ECCN 3A991.b.2.a – 每封裝存儲容量超過1 Mbit的靜態隨機存取存儲器 (SRAM)。參閱美國商務部工業和安全局，「商業管制清單：第3類——電子產品」。

150 由第三方商業供應商提供的貿易數據。

151 Ibid.

值得注意的是，其中90%以上是由總部位於瑞士的NVS Technologies AG運到KB NAVIS的，這兩家公司皆為NAVIS集團公司的子公司。[152]

NVS Technologies的首席執行官是一位名叫Vasiliy Engelsberg的俄羅斯人，[153] 他也是KB NAVIS[154]和整個NAVIS公司集團的聯合創始人。[155] 此外，KB NAVIS 聯合創始人Valery Babakov[156]還擔任了金剛石-安泰消費者導航設備的首席設計師。[157] Babakov在2008年與Engelsberg合著的一篇關於GLONASS商業化的文章中指出， NAVIS集團是俄羅斯GLONASS接收器的主要供應商。他還解釋說，NVS技術公司的成立是「作為我們的技術融入全球GNSS市場進程的努力的一部分」。[158]

雖然KB Navis似乎製造多種民用應用，但2019年的俄語行業報告稱，該研究所70%以上的合同是與俄羅斯國防部簽訂的。[159] 當時，這些業務明顯已經超過35億盧布，即5500萬美元。因此，KB NAVIS公司進口的許多來自西方的零部件很可能進入了本報告所評估的俄羅斯武器系統。

152 「Nekommercheskaya organizaciya Associaciya razrabotchikov, proizvoditelei i potrebitelei oborudovaniya i prilozhenij na osnove global’nyh navigacionnyh sputnikovyh sistem GLONASS/GNSS-Forum」【以全球衛星導航系統GLONASS/GNSS-Forum為基礎的設備和應用開發者、製造商和消費者協會的非商業組織】，「Analiticheskij otchet po itogam izsledovaniya sostoianiya i perspektiv razvitiya rynka navigacionnyh, svyazanyh i navigacionno-sviazannyh modulej, a takzhe ocenki vliyanniya na razvitie rossijskogo I mezhdunarodnogo rynka “Avtonet”」【關於導航、網絡和導航網絡模塊市場狀況和發展前景的研究結果的分析報告，以及對俄羅斯和國際「Autonet」市場發展的影響評估】，第187頁、160頁。

153 領英，‘Vasily Engelsberg’，<https://ch.linkedin.com/in/vasily-engelsberg-3b637b16>，訪問日期2022年7月21日。

154 Polina Jeremenko，「Soshel s orbity」［離開軌道］，Moskovskiye Novosti［莫斯科新聞］，2011年4月7日，<https://www.mn.ru/politics/68113>，2022年7月3日。

155 PravoRU，‘Sobstvenniku postavschika Minoborony otkazali v iske na sovladel’ca’［國防部供應商的所有人對共同所有人的索賠被拒絕］，2017 年 11 月 10 日，<https://pravo.ru/news/view/145748/>，2022年7月3日。

156 Ibid.

157 Novosti navigacii，「第五屆國際衛星導航論壇」，（2011年第2期），第51頁，<Https://internavigation.ru/wp-content/uploads/2019/07/nn2011_02.pdf#page=51>，訪問日期2022年7月12日。 <

158 Vasiliy Engelsberg，Ivan Petrovski及Valery Babakov，「專家建議：GLONASS業務前景，GPS世界，2008年3月1日，<https://www.gpsworld.com/gnss-systemglonassexpert-advice-glonass-business-prospects-4215/>，訪問日期2022年7月21日。

159 根據這份文件，KB NAVIS與俄羅斯聯邦政府簽訂了106份價值51億盧布的合同。其中20份合同價值36億盧布，公司業務的72.6%是與俄羅斯國防部簽訂的。‘Nekommercheskaya organizaciya Associaciya razrabotchikov, proizvoditelei i potrebitelei oborudovaniya i prilozhenij na osnove global’nyh navigacionnyh sputnikovyh sistem GLONASS/GNSS-Forum’［以全球衛星導航系統 GLONASS/GNSS-Forum 為基礎的設備和應用開發者、製造者和消費者協會的非商業組織］，‘Analiticheskij otchet po itogam izsledovaniya sostoianiya i perspektiv razvitiya rynka navigacionnyh, svyazanyh i navigacionno-sviazannyh modulej, a takzhe ocenki vliyanniya na razvitie rossijskogo i mezhdunarodnogo rynka “Avtonet”’［關於導航、網絡和導航網絡模塊市場狀況和發展前景的研究結果的分析報告，以及對俄羅斯和國際「Autonet」市場發展的影響評估］，第189頁。

KH-101巡航導彈

Kh-101 ALCM已在烏克蘭被大量使用。該導彈已被用於攻擊各種目標，包括鐵路基礎設施[160]和城市中心。[161] 值得一提的是，自20世紀80年代以來，該設計就一直在被討論中，但由於缺乏國家資金，其投入使用的速度放緩，開發工作也被推遲到了2000年代。[162]

該導彈於2012年投入使用，是一種遠程防區外巡航導彈，射程可達2,800公里，可攜帶常規彈頭，如高爆彈、碎片彈、子彈藥，甚至250節核彈頭。它可從飛機上發射，無需助推器獲得初始速度，據報導可以在6,000米的高度以 0.58 馬赫的速度巡航。[163] 此外，該導彈可以0.78馬赫的最高速度飛向30-60米高度的目標。[164]

它使用一系列系統和傳感器進行中段導航，包括慣性、GLONASS和GPS衛星數據。[165] 後面的這幾個信號由安裝在9M727巡航導彈上的同一個SN-99（ＣＨ-99）單元接收和處理。光電校正系統採用存儲的地形圖進行地形比較更新。[166] 在其最終階段，Kh-101使用了電視成像紅外導引頭。[167]

160 國防部（@DefenceHQ），「(2/6) 6月5日凌晨，俄羅斯Kh-101空射巡航導彈襲擊了基輔的鐵路基礎設施，可能是為了擾亂西方軍事裝備對烏克蘭前線部隊的供應」，推特，2022年6月6日，<https://twitter.com/DefenceHQ/status/1533682058463268864>，訪問日期2022年7月21日。

161 美国国家广播公司新闻网，「據報導，俄羅斯導彈數週來首次襲擊基輔，造成2人死亡」。

162 Robin Hewson，「俄羅斯最新巡航導彈的細節浮出水面」，簡氏防務周刊，2007年10月，<https://web.archive.org/web/20080225163154/http://www.janes.com/news/defence/systems/jdw/jdw071022_1_n.shtml>，訪問日期2022年7月21日。

163 CSIS導彈防禦項目，‘Kh-101 / Kh-102’，2021 年 7 月 31 日，<https://missilethreat.csis.org/missile/kh-101-kh-102/>，訪問日期2022年7月21日。

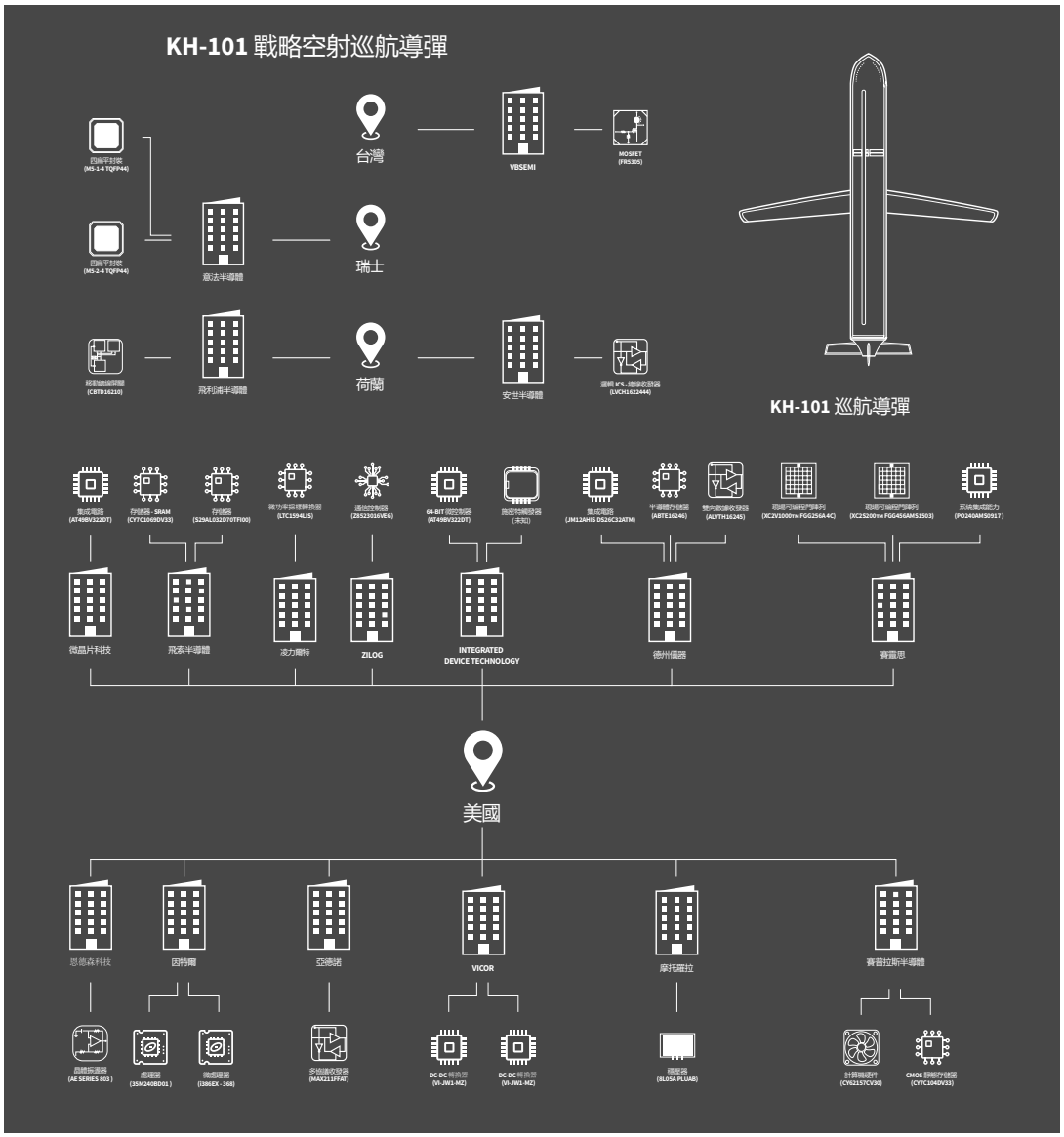
164 Ibid.

165 Ibid.

166 Ibid.

167 Ibid.

Figure 20: Kh-101中的西方零部件



來源：RUSI.

從被找到的完整Kh-101導彈可以看出它至少有六個子系統，比如衛星導航系統、一套接收器單元、一個處理器模塊和一個計算單元。所有這些系統都安裝了大量的由西方製造的微電子元件。例如，BT33-202處理器模塊有至少十幾個微電子元件，包括CMOS SRAM模塊、FPGA、RS-232和總線收發器，全都是由美國和荷蘭的一系列公司製造的。特別是還包括德州儀器製造的CMOS四路差分線路接收器，它能在保持低功耗特性的同時進行平衡和非平衡數字數據傳輸。德州儀器聲明該零部件是按照美國Mil-Std-883C規範製造的，但該產品卻屬 EAR99 類產品。[168]

168 德州儀器 DS26C32ATM/NOPB - CMOS 四路差分線路接收器，<https://www.ti.com/product/DS26C32AT/part-details/DS26C32ATM/NOPB>，訪問日期2022年7月21日。

漏洞：零部件流入俄羅斯

儘管多年來為了限制俄羅斯軍方獲得關鍵零部件而施加的製裁和出口管制日益嚴格，但俄羅斯在2017年至2021年間貨運級貿易記錄和進口申報單為這些零部件究竟是如何進入俄羅斯提供了些答案。[169]

利用這些記錄和一種叫做Altana Atlas的工具，研究團隊篩查了數十億份俄羅斯進口半導體和半導體相關產品的協調貿易記錄，這些進口產品可能被用在襲擊烏克蘭的俄羅斯武器平台上。[170]

研究團隊又對該數據集進行檢查，找出有哪些實體被作為這些零部件順利進入俄羅斯軍工複合體的渠道，在這一過程中我們找出了幾十家軍事進口商和其他與俄羅斯國防工業有密切聯繫的公司。

全球供應鏈：俄羅斯半導體進口

俄羅斯是商業用途、工業用途和軍事用途的半導體和微電子產品的進口大國。為了更好地了解這些產品的供應情況，研究團隊搜索了2017-22年俄羅斯公司用與微電子和微電子相關商品相對應的HS編碼的所有商品進口交易。[171]

169 由 Altana Trade Atlas (https://altana.ai/atlas/) (https://altana.ai/atlas/) 和第三方商業數據提供商提供的貿易數據。

170 Altana Trade Atlas, <https://altana.ai/atlas/>.

171 HS編碼，即協調制度編碼是用於表示國際貿易中商品類別的標準化編碼。HS編碼代表商品類別，但不具體到產品。前六位數字是國際標準化的，六位數之後由各個國家根據自己的記錄目的進行修改。在我們的樣本中納入了HS編碼「854239」（電子集成電路；其中元件），「854129」（未安裝的芯片、裸片和晶圓），「'854110」（二極管，不包括光敏或發光二極管），「854231」（處理器和控制器，無論是否與存儲器、轉換器、邏輯電路、放大器、時鐘和定時電路或其它電路相結合）和「381800」（摻雜在電子產品中使用的化學元素，形式為圓片、晶圓或其它類似形式）。

03

該過程幫助我們找出了那一时期俄羅斯进口的近100萬件與半導體相關的产品。[172] 共有5,597家不同的進口公司。這些公司種類五花八門，從大型、多投入批發品加工商到專業的電子產品製造商，從僅僅進行公司內部貿易的西方跨國公司的地方分支機構到公司專門與俄羅斯軍工复合体打交道的公司。Altana Atlas找出的交易內容無所不包，從用於簡單台式電腦的半導體，到在烏克蘭戰場上發現的精確類型的高度專業化零部件。[173]

不出所料，按總交易數量計算，最大進口商往往是從世界各地採購各種電子元件的批發進口商。

Figure 21: 俄羅斯最大進口商

進口商	半導體相關交易數	
OOO BELIV	100,313	德國 – 8,544 馬來西亞 – 7,403 中國 – 7,213 菲律賓 – 4,037 美國 – 3,880
KOMPONENT	34,252	美國 – 12,884 馬來西亞 – 3,088 中國 – 2,732 香港特別行政區 – 1,943 泰國 – 1,850
BALTELEKTRON	32,377	美國 – 9,025 英國 – 5,357 香港特別行政區 – 3,931 中國 – 2,635 馬來西亞 – 2,449
WEST-OST	29,115	德國 – 6,018 香港特別行政區 – 4,830 中國 – 4,763 馬來西亞 – 2,085 台灣 – 1,389
SPETSVOLTAZH	28,843	中國 – 6,576 芬蘭 – 5,637 美國 – 3,449 馬來西亞 – 2,654 台灣 – 2,241

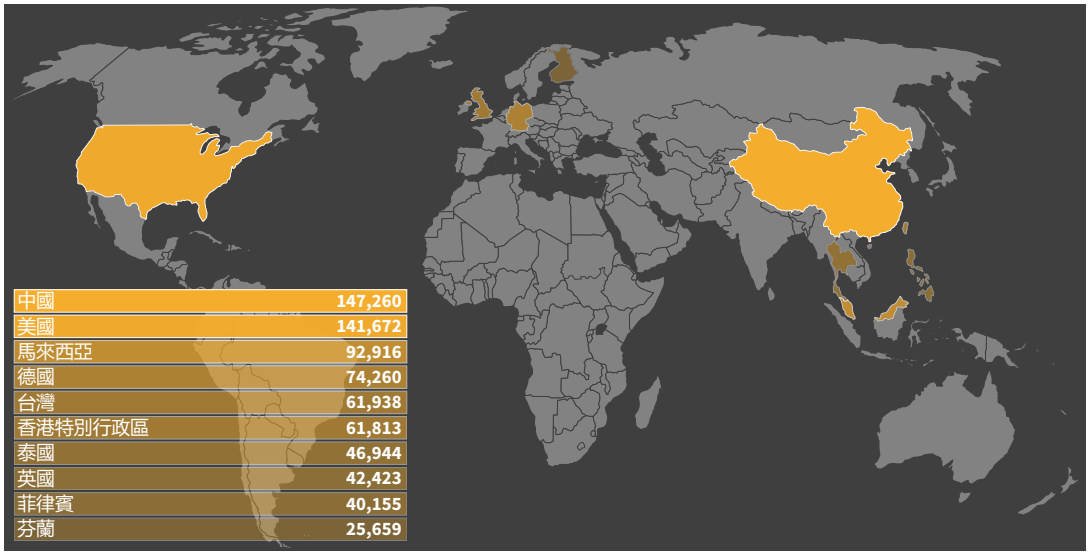
來源： Altana Atlas; RUSI.

172 Altana Trade Atlas.

173 Ibid.

電子產品來自多個國家和司法管轄區。中國、美國、德國、台灣、香港和英國等主要的半導體出口管轄區都在前10大供應商之列，但還有大量的交易來自馬來西亞和泰國等國家。而許多大型跨國半導體製造商都在這些國家設有製造廠和設施，他們通常將組裝完的集成電路在这里进行测试，然後再運往客戶和分銷商。[174]

Figure 22: 供給俄羅斯的前10大半導體和微電子出口商



來源：Altana Atlas; RUSI.

然而，更仔細研究後发现，其中一些交易產品，尤其是那些來自半導體和電子行業不發達的國家的交易產品，通常不太可能是由該國家交貨的製造商所製造的。對於這類交易，一般有兩種解釋：退貨和轉運。

檢驗退貨真實性，通常可以通過檢查交易中涉及的交易對手的性質來實現。例如，Altana Atlas展示了所研究的時間段裡從阿爾及利亞發貨到俄羅斯的半導體相關商品的幾筆交易。從詳盡的交易數據可以看到，所有這些貨物都是從阿爾及利亞國防部發給PAO Kompaniya Sukhoi和PAO Kompaniya Irkut（兩家著名的俄羅斯國防承包商）的非發光二極管和集成電路。[175]

由於阿爾及利亞軍方使用這兩家公司製造的防禦系統，[176] 這些交易產品很可能不是阿爾及利亞國防部製造的成品微電子產品，而是有缺陷、多餘或其它不需要的零部件的退貨。從那些缺乏強大電子製造業卻向俄羅斯發貨的其它國家的公司那裡，也觀察到了類似的交易現象。

通過第三國轉運的情況對調查工作更重要但也更具挑戰。微電子第三方分銷商和批發商通常在香港等中間司法管轄區開展業務，這意味着運往俄羅斯的零部件有時是通過位於俄羅斯境外的貿易實體合法供應的。然而，採購代理經常會利用第三國掩蓋真正的出口商或終端用戶來轉移敏感和受管制貨物。[177] 俄羅斯的秘密採購網絡和代表他們行事的個人與企業往往將其業務設在擁有大

174 Ibid.

175 Sukhoi是著名的軍用品牌，於2022年2月24日併入俄羅斯聯合飛機公司（United Aircraft Corporation），該公司於2022年2月24日得到英國製裁。見英國外交、聯邦和發展辦公室，「外交大臣實施英國最嚴厲的製裁，對俄羅斯造成最大和持久的痛苦」，新聞稿，2022年2月24日，<https://www.gov.uk/government/news/foreign-secretary-imposes-uks-most-punishing-sanctions-to-inflict-maximum-and-lasting-pain-on-russia>，訪問日期2022年7月21日。 Kompaniya Irkut的許多子公司和附屬公司都被列入美國財政部指定名單。參閱美國財政部，「俄羅斯相關指定名單和指定名單更新； 與俄羅斯有關的一般許可證頒發和相關常見問題」，新聞稿，2022年6月28日，<https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220628>，訪問日期2022年7月21日。

176 Times Aerospace，「阿爾及利亞將從俄羅斯獲得14架SU-57戰鬥機」，<https://www.timesaerospace.aero/news/defence/algeria-to-get-14-su-57-fighters-from-russia>，訪問日期2022年7月10日。

177 Daniel Salisbury，『探索在擴散網絡中使用「第三國」：馬來西亞案例』，歐洲國際安全雜誌（第4卷，第1期，2019年2月）。

型微電子貿易行業且管制又松的司法管轄區。例如，就在2022年6月28日，三名個人和一家名為EMC Sud Limited的香港公司因受到參與與FSB關聯的秘密採購網絡的指控而遭到OFAC的制裁。其中一人是前FSB特工Alexander Kokorev，被控幫助俄羅斯的國防工業基地秘密從美國、日本和歐洲採購電子產品。[178]

從轉運模式角度開展調查具有挑戰性，主要是因為這需要摸清多層次的貨物運輸情況，包括原產國出發情況、經過過境國情況，以及最後到達目的地國的情況。儘管很難識別轉運，但Altana Atlas等工具可以幫助我們洞悉包含多個階段的整個價值鏈，進而找出哪些交易屬於轉運。

例如，位於印度新德里的半導體製造商SP半導體私人有限公司（SP Semiconductors Private Limited）於2021年6月9日向金派科技（香港）有限公司（King-Pai Technology (HK) Co Ltd）運送了英飛凌（Infineon）品牌的集成電路。同月晚些時候，金派向幾家活躍在軍工領域的俄羅斯公司發送了多筆具有相似描述的商品交易，這些俄羅斯公司包括Trade-Component[179]和Radiant Electronic Components（兩公司均於 2021首次受到美國財政部的製裁），[180] 以及Radioavtomatika公司（於2022年首次受到制裁）。[181] 所有公司都有向俄羅斯軍方提供微電子產品的歷史記錄。[182] 金派科技因支持俄羅斯的軍事和國防工業於2022年6月下旬被添加到BIS的實體清單中。[183] 該公司的香港公司記錄中顯示名叫姚金標的中國公民為該公司的唯一董事和股東。根據該公司網站的存檔版描述，該公司在俄羅斯莫斯科和越南胡志明市設有海外辦事處。[184] 姚金標似乎還使用「金派」名字經營另一家香港公司，一家是金派科技國際有限公司（Kingpai Technology International Co Ltd），直接由其經營，而另一家名稱相似的金派科技集團有限公司（Kingpai Technology Group Co Ltd）則由與其同姓，即也姓姚的人士經營。[185]

178 美國財政部，「美國財政部對普丁戰爭機器中的近100個目標進行制裁，禁止俄羅斯進口黃金」，新聞稿，2022年6月28日，〈https://home.treasury.gov/news/press-releases/jy0838〉，訪問日期2022年7月22日。

179 Altana Trade Atlas, 〈https://altana.ai/atlas/〉.

180 美國商務部工業與安全局，「在實體清單中增加某些實體；修訂實體清單中的現有條目；從未經核實的清單中刪除實體；在軍事終端用戶（MEU）清單中增加實體」，2021年7月12日。〈https://www.federalregister.gov/documents/2021/07/12/2021-14656/addition-of-certain-entities-to-the-entity-list-revision-of-existing-entry-on-the-entity-list〉, 訪問日期2022年7月22日。

181 美國財政部，「俄羅斯關聯的指定名單； 與俄羅斯關聯的通用許可證的頒發」，新聞稿，2022年3月3日，〈https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220303〉, 訪問日期 2022年7月22日。

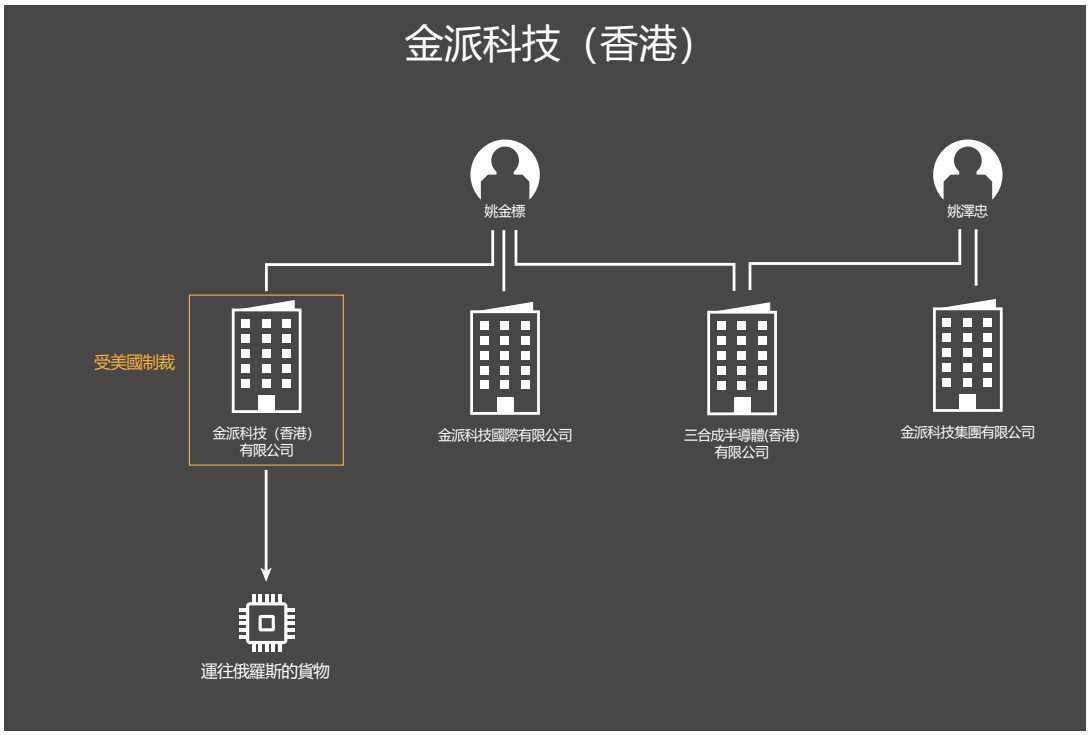
182 Alexandra Alper，「美國指控中國五家公司支持俄羅斯軍隊」，路透社，2022年6月29日。

183 美國商務部工業和安全局，《第744部分的第4號補充 - 實體清單》，2022年6月28日， 〈https://www.bis.doc.gov/index.php/documents/regulations-docs/2326-supplement-no-4-to-part-744-entity-list-4/file〉,，訪問日期2022年7月22日。

184 金派科技（香港）有限公司, 「聯繫我們」, 〈https://www.king-pai.com/contact.asp〉, 訪問日期2022年7月22日。

185 香港公司註冊處，可瀏覽〈www.icris.cr.gov.hk〉。

Figure 23: 金派網絡旗下公司



來源：美國工業和安全局； 香港公司註冊處； 企查查； Altana Trade Atlas； RUSI。

對姚金彪的董事身份搜索顯示，他經營着一個涉及微電子銷售的公司網絡，以深圳一家名為深圳市三合成科技有限公司為該網絡的核心企業。[186] 根據Altana Atlas，三合成科技的出口歷史記錄在很大程度上與金派十分相似，貿易記錄顯示，他們與Radioavtomatika和Trade-Component等受制裁實體進行了幾筆微電子和相關貨物的交易。[187]

深探戰場

另一項研究工作是詳細研究與戰場上發現的俄羅斯武器系統相關的貨物和零部件的確切運輸情況。

研究小組把從俄羅斯武器系統拆卸下來的204個半導體序列號作為樣本，借助Altana Atlas搜索所有與這204個樣本相匹配的出口到俄羅斯的交易。總共找出2,744批與這批序列號樣本匹配的貨物，被發往俄羅斯的286位唯一收貨人。[188]

186 企查查，深圳市三合成科技有限公司，<https://www.qcc.com/firm/535b9127d06edbbba894ca64b6ae41b6.html>，訪問日期2022年7月22日。

187 Altana Trade Atlas，<https://altana.ai/atlas/>。

188 Ibid.

許多半導體有多種用途，即便搜索到的貨物與在俄羅斯武器系統裡找到半導體產品類型完全相同，該半導體貨物也可能屬民用。其中幾批貨物可能確實是被用於正道，但很巧的是，同樣這幾批半導體居然也用在俄羅斯武器上。事實上，Altana Atlas找出了幾家西方公司向其俄羅斯子公司發送半導體的公司內部交易的例子。在這些情況下，故意轉移到軍隊的可能性很低。[189]

然而，其他進口商構成了更高的風險。例如，ZAO Radiotekhkkomplekt (RTKT) ——一家長期向軍方供貨的公司，在數據庫中以收貨方出現，接收的貨物是半導體產品，與在俄羅斯武器中找到半導體類型完全相同。這些半導體的製造商包括TE Connectivity、Microchip Technology、亞德諾半導體科技公司子公司凌力爾特公司和許多其它公司。[190] RTKT成立於1997年，為一些俄羅斯企業、研究機構和設計局供應電子元件。[191] 同時，根據RTKT網頁的存檔版本介紹，該公司自2000年以來已獲得向軍方提供某些類型電子元件的認證，[192] [193] 並聲稱俄羅斯直升機製造商Kumertau Aviation Production Enterprise (AKA AO KUMAPP) 至少在2020年之前是其客戶之一，該公司被美國指定為制裁對象。[194] 該網頁還介紹了RTKT是德州儀器、賽普拉斯半導體、Golledge等一系列西方科技公司的供應商，[195] 而這些公司的零部件經常出現在俄羅斯的武器系統中。

與此同時，其他幾家公司也接收了與在烏克蘭戰場上找到的零部件完全相同的貨物，比如Rosoboronexport和Uralvagonzavod，這些公司已經成為各種西方制裁的目標。[196]

追踪受制裁實體

除了研究那些經確認最終出現在戰場上的半導體產品，我們還可以追踪那些代表俄羅斯軍隊參與技術轉讓，而被美國及其盟國公開制裁的實體的供應鏈。許多製裁是最近實施的，這意味着Altana Atlas顯示的歷史交易記錄在發生交易時也許並不違法。即使交易在進行時是合法的，這些公司的交易活動也可以讓我們窺探到其採購網絡的真實性質。

再回到幫助俄羅斯進口微電子產品的5,597家公司的原始樣本，研究小組從四十多家公司的記錄中發現，這些公司亦或直接出現在美國和國際制裁或出口管制名單上，亦或被制裁名單上公司擁有50%股份（因此受法律制裁）。[197]

在樣本中，接收半導體相關進口貨物的被拒貿易方包括那些因替俄羅斯軍隊採購電子產品而被制裁的公司，包括Npo Elektronnye Sistemy、Radioavtomatika、Publichnoe Aktsionernoe Obshchestvo Oplot和許多其他公司。根據Altana Atlas，直接被拒或根據法律被拒的貿易方的交易一直持續到2021年9月，這也許說明交易對手可能成功逃避制裁或盡職調查工作失職。[198]

通過更詳細地檢查某個公司的進口歷史記錄，能夠逐步了解它們是如何充當這些商品進入俄羅斯軍事系統的渠道的。例如，Altana Atlas向我們展示了PAO Mikron與來自33個國家和司法管轄區（包括美國、英國、德國、荷蘭和台灣）的148個不同發貨人之間的2,500多筆個人貿易交易。如前所述，Mikron一直是蘇聯集成電路的主要製造商

189 Ibid.

190 Ibid.

191 Radiotekhkomplekt, 「主頁」, <http://web.archive.org/web/20161219070553/https://www.rtkt.ru/eng/>, 訪問日期2022年7月22日。

192 美國財政部，「U.S. 財政部製裁俄羅斯國防工業基地、俄羅斯杜馬及其成員以及Sberbank首席執行官」，新聞稿，2022年3月24日， <https://home.treasury.gov/news/press-releases/jy0677>, 訪問日期2022年7月22日。

193 Radiotekhkomplekt, 「關於」。

194 Ibid.

195 Radiotekhkomplekt, 「製造商」, <https://www.rtkt.ru/eng/manufacturers/>, 訪問日期2022年7月22日。

196 美國財政部，「烏克蘭-俄羅斯相關聯的指定名單和識別更新； 敘利亞制裁指定名單； 主銷法案指定名單； 烏克蘭/俄羅斯相關的通用許可證12和13的頒發； 新常見問題解答和更新的常見問題解答發布”，新聞稿，2018年4月6日，<https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20180406>，訪問日期2022年7月22日。

197 美國財政部，「特別指定國民和被禁人員名單 (SDN) 可讀名單」，2022年6月28 日， <https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists>, 訪問日期2022年7月22日。

198 Altana Trade Atlas, <https://altana.ai/atlas/>。

之一，並且仍然在營銷詞中把自己描述成俄羅斯領先的微電子製造商和出口商。[199] 據說該公司於2016年簽訂了為俄羅斯航天運載火箭製造電子元件的合同。[200] Mikron已因與俄羅斯入侵烏克蘭相關聯而受到美國財政部的製裁。[201]

提及的2,500筆交易幾乎全部都是半導體相關的製造設備或零部件。包括Mikron與一家愛爾蘭公司之間的一項交易，該交易涉及ASML製造的Twinscan XT:1060k光刻激光系統中用到的部分激光器，該系統用於製造集成電路。[202] 來自英國一家公司的另一筆交易提到了「洗淨的單晶摻雜矽板經拋光用於微電子」。[203] 雖然這些交易在進行時可能違反了也可能未違反制裁，但確實讓產品更容易流入俄羅斯軍工複合體，從而也更容易流入烏克蘭戰場。

香港芯片店

2022年6月，BIS將幾家支持俄羅斯軍事和國防工業基地[204]的非俄羅斯公司列入了實體清單，實際上禁止了這些公司從美國進口和再進口乃至EAR99類別的貨物。

其中包括一家總部位於香港的信諾電子科技有限公司，（Sinno Electronics Co Ltd或Xinnuo Electronic Technology），該公司在中國內地的香港和深圳設有多個經營處。[205][206] 公司所有人和經營者為三位中國公民，他們的名字分別為彭敏波（別名Betty Peng）、林青 （別名 Becky Lin），及洪俊旭（別名 Billy Hong；又名阿旭）。[207]

信諾在線業務強大，不僅有網店，還有一個全英文網站專門[208] [209]推銷亞德諾半導體技術、德州儀器和許多其他製造商的產品。[210] 該公司似乎至少從2013年就開始參加在莫斯科舉辦的俄罗斯国际电子元器件及设备展览会（ExpoElectronica），[211] 最近一次參加是在2021年。[212] 在新冠疫情期間，該公司甚至贊助了2020年「中俄在高科技領域的合作」網絡研討會。[213]

199 Mezhdunarodnyj Ob’yedinnenyj Biographicheskij Centr [國際聯合傳記中心]，『Nacional’noe dostoyaniye, OAO 「NIIME i Mikron」』’ [國家寶藏, OJSC 「NIIME 及 Mikron」]，<http://www.biograph.ru/index.php/nationdestiny/5269-mikron>，訪問日期2022年7月25日；Mikron，「Mikron 歷史」，<https://en.mikron.ru/company/history/>，訪問日期2022年6月30日；Mikron，<https://en.mikron.ru/>，訪問日期2022年6月30日。

200 ZZelenograd Infoportal，『「Mikron」 zaimetsya proizvodstvom elementov noveyshey sistemy upravleniya dlya raket-nositele』（「Mikron」將為最新的太空運載火箭控制系統製造元件），2016年12月7日，<https://www.netall.ru/society/news/983044.html>，訪問日期2022年7月25日。

201 美國財政部，「財政部瞄準制裁規避網絡和支持普丁戰爭的俄羅斯科技公司」，2022年3月31日，<https://home.treasury.gov/news/press-releases/jy0692>，訪問時間22年7月27日。

202 Altana Trade Atlas，<https://altana.ai/atlas/>。

203 Ibid.

204 美國商務部工業與安全局，「實體添加、條目修訂及更正以及從實體清單中刪除實體」，2022年6月30日。<https://www.bis.doc.gov/index.php/documents/federal-register-notices-1/3043-public-display-version-of-entity-list-rule-on-public-display-and-effetive-6-28-22-scheduled/file>，訪問日期2022年7月22日。

205 信諾電子科技，「聯繫我們」<http://www.sinnoelec.com/contact.aspx>，訪問日期2022年7月22日。

206 美國商務部工業和安全局，「聯邦公告/第 87 卷，125 號」，2022年6月30日，<https://www.bis.doc.gov/index.php/documents/regulations-docs/federal-register-notices/federal-register-2022/3053-87-fr-38920-entity-list-rule-effective-6-28-22-published-6-30-22/file>，訪問日期2022年7月22日。

207 香港公司註冊處，<www.icris.cr.gov.hk>。

208 香港目錄，「信諾電子科技有限公司」，<http://hksinno.hkinventory.com/Shop/Page_CompanyProfile.asp>，訪問日期2022年7月22日。

209 信諾電子科技，「主頁」，<http://www.sinnoelec.com/index.aspx>，訪問日期2022年7月22日。

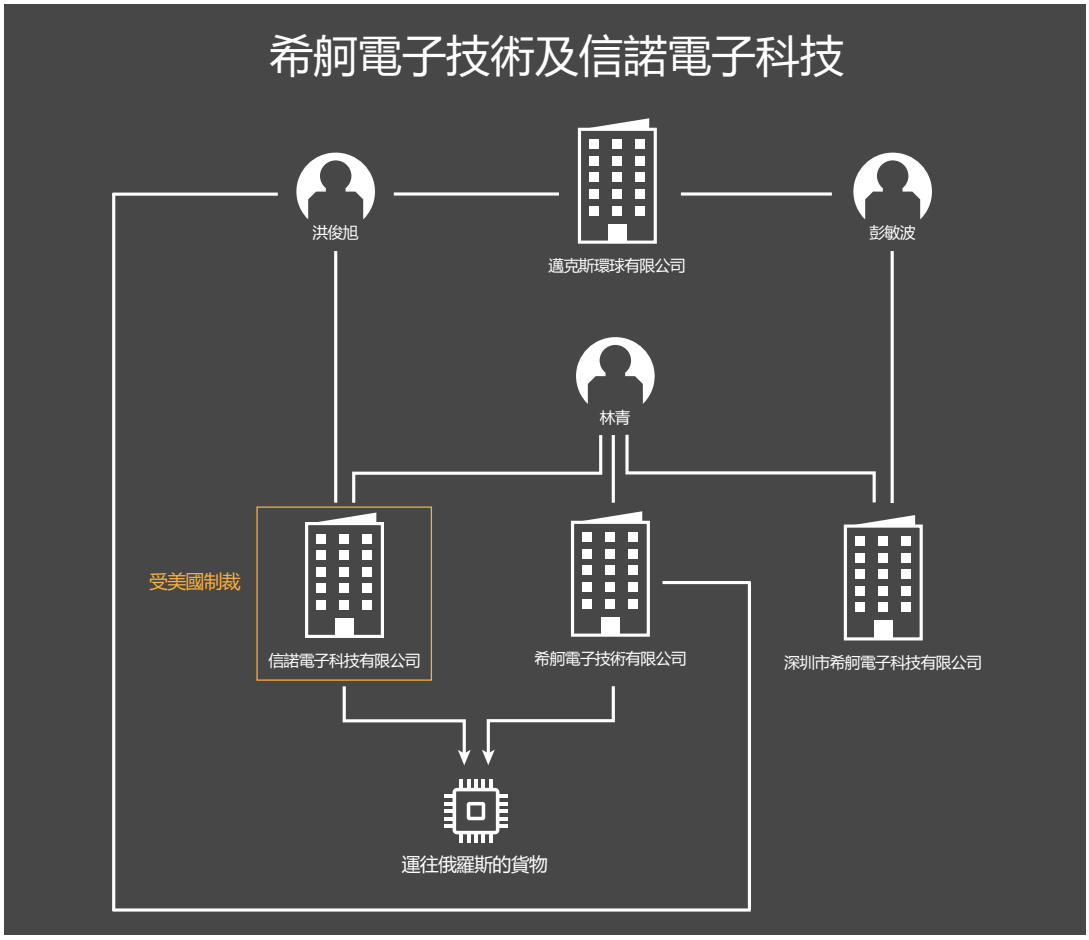
210 信諾電子科技，「聯繫我們」，<http://www.sinnoelec.com/product.aspx>，訪問日期2022年7月22日。

211 香港目錄，「俄羅斯國際電子元器件及設備展覽會（Expo Electronica），2013年4月10-12日，莫斯科」，<https://www.hkinventory.com/public/UpcomingEventDetail.asp?id=173>，訪問日期2022年7月22日。

212 俄羅斯國際電子元器件及設備展覽會，「領先的製造商、供應商和客戶將在俄罗斯国际电子元器件及设备展览会匯集並現場互動」，新闻稿，2021年4月6日，<https://expoelectronica.ru/Articles/press-release-en-ee-2021>，訪問日期2022年7月22日。

213 俄羅斯國際電子元器件及設備展覽會，「中俄合作」<https://expoelectronica.ru/Page/russia-china-forum>，訪問日期2022年 7月22日。

Figure 24: 信諾與希舸網絡



來源：美國工業和安全局； 香港公司註冊處； 企查查； Altana Trade Atlas； RUSI。

信諾的網店裡列出了其零部件的最新庫存。[214] 總共43個現貨零部件中，有20個被BIS列為出口管制產品。特別是這些受管制零部件中有許多是由NXP、德州儀器和意法半導體這些主要的微電子製造商製造的。事實上，其中一個由意法半導體公司製造的STM32F103VCT6微控制器，[215] 正是從俄羅斯軍隊在烏克蘭部署的Orlan-10無人機上發現的型號。

根據貿易記錄和進口報關顯示，在2017年至2021年期間，信諾向各種俄羅斯公司出口了大量半導體和微電子產品。[216] 其中之一是總部位於莫斯科的000 Trade-Component，於2021年7月12日受到美國政府的製裁，原因是其涉嫌「參與可能有助於推進俄羅斯的軍事計劃美國原產電子元件採購活動」。[217]

信諾向000 Trade-Component發運的最後一批貨似乎是在2021年6月，當時這家香港供應商向莫斯科發運了價值超過10萬美元的亞德諾半導體科技公司品牌的電子集成電路。[218]

214 香港庫存，「信諾電子科技有限公司」，<http://hksinno.hkinventory.com/Shop/Page_Inventory.asp>，訪問日期2022年7月22日。

215 Ibid.

216 由第三方商業供應商提供的貿易數據。

217 美國商務部工業與安全局，「在實體清單中增加個別實體；修訂實體清單中的現有條目；從未經核實的清單中刪除實體；在軍事終端用戶（MEU）清單中增加實體」，聯邦公告，2021年7月12日。<https://www.federalregister.gov/documents/2021/07/12/2021-14656/addition-of-certain-entities-to-the-entity-list-revision-of-existing-entry-on-the-entity-list> 訪問日期2022年7月10日。

218 由第三方商業供應商提供的貿易數據。

然而，香港公司記錄顯示，Becky Lin和Billy Hong在當地註冊了另一家公司，名為希舸電子技術有限公司（Sigma Technology Limited），[219] 該公司一直向俄羅斯運送大量微電子及相關商品。[220] 根據2018年4月至2021年6月提交的貿易記錄，該公司向俄羅斯運送了價值超過300萬美元的貨物，是姊妹公司信諾電子科技在同期內向俄羅斯運送貨物的七倍多。[221]

希舸電子技術在2014年[222]俄羅斯入侵克里米亞後僅兩個月就成立了，似乎只向少數客戶發貨。其中之一就是上文提到的RTKT，該公司在2017年2月至2021年12月期間從希舸接收了數百批微電子產品。[223] 奇怪的是，信諾的貿易記錄沒有記載信諾在2017年至2021年期間向俄羅斯運送過任何意法半導體品牌的元件，但在同一時期，希舸至少向RTKT運送了35批該品牌的元件。[224]

另外值得注意的是，希舸還向其他軍事供應商供應微電子產品，例如AO Radiopriborsnab，[225] 一家電子元件供應商，是受制裁（俄羅斯國家技術集團為母公司）的康採恩無線電電子技術（Concern Radioelektronnye technologii，或 CRET）的子公司。

219 香港公司註冊處，<www.icris.cr.gov.hk>。

220 由第三方商業供應商提供的貿易數據。

221 Ibid.

222 香港公司註冊處， <www.icris.cr.gov.hk>。

223 由第三方商業供應商提供的貿易數據。

224 Ibid.

225 Altana Trade Atlas, <https://altana.ai/atlas/>。

結論

在俄羅斯入侵烏克蘭和隨之實施的國際制裁之後，俄羅斯總統府成立了一個委員會，專門研究俄羅斯國防工業如何能夠維持關鍵軍事系統的生產。俄羅斯科學院的幾個實驗室和主要的國有軍事企業負責評估了他們是否可以在俄羅斯製造零部件，是否可以將目前已被制裁的零部件更換成由供應未受管制的國家製造的替代品，或者是否有必要規避制裁。評估結果並不容樂觀。為了讓俄羅斯武器使用外國採購的零部件，製造商必須向俄羅斯國防部證明為什麼必須使用該零部件。製造商還必須解釋為什麼它不能以商業可行的方式在俄羅斯製造，為什麼不能用來自友好國家的替代零部件，以及為什麼使用該零部件不會破壞設備的安全性。軍用通信系統的具體架構還必須得到負責確保俄羅斯加密安全性的FSB的批准。簡而言之，本報告中詳述的俄羅斯武器系統中發現的絕大多數外國製造的零部件對這些系統的可行性來說是至關重要的。

歷來，俄羅斯特殊事物部在維持西方微電子產品供應方面取得了巨大成功。他們在冷戰期間獲得了大量零部件，在冷戰制裁解除後還大幅擴大了對這些商品的採購幅度。在許多情況下，俄羅斯軍方提前為關鍵系統採購了至少可用十年的零部件庫存，為供應不受制裁影響而防患於未然。然而，很明顯，他們並沒有在本報告中找到的所有零部件上都能實現這一目標。鑑於俄羅斯已經搭建了一個對國際安全構成重大威脅的複雜的武器庫，並在烏克蘭表明俄羅斯政府對使用這些武器進行侵略戰爭（包括故意以平民為目標）毫無忌憚。為了阻止俄羅斯填補其庫存，未來的製裁和執法力度至關重要。

俄羅斯為軍事目的採購西方微電子產品的大部分情況下依靠虛假的終端用戶證書、幌子公司和轉運等手段。詳細了解和關閉這些網絡是遏制俄羅斯國防工業的第一步，但由於俄羅斯在重組其採購架構的過程以違反《維也納公約》的做法轉移用欺詐手段採購的零部件，並試圖賄賂或滲透入監管機構，未來要阻止將此類零部件運往俄羅斯還需依賴高度持續性的監管。此外，很明顯的是，由於第三國被廣泛用來轉運零部件以供後續銷售，要限制俄羅斯國防工業還需要大量的國際合作。

如何應對俄羅斯因無法獲得複雜武器的關鍵零部件而導致的意外後果也很重要。許多國家依賴俄羅斯為他們供應武器。保證能獲得這些武器对這些国家的安全十分重要。比如像對印度這樣45%的國防進口來自俄羅斯的國家來說，[226]得不到俄

226 經濟時報，「俄羅斯對印度武器出口份額从2012-17年的69%下降到2017-21年的46%：報告」，2022年3月15日。<https://economictimes.indiatimes.com/news/defence/russias-share-of-arms-import-to-india-fell-from-69-in-2012-17-to-46-in-2017-21-report/articleshow/90218483.cms>，訪問日期2022年7月10

日。 羅斯設備會威脅到他們的國家安全。這可能會促使那些處於如此境地的國家為俄羅斯逃避制裁提供便利。不過，由於處於這一境地的國家很少有大型微電子產業，這可能會促使這些國家改變供應商。如果西方聯盟能夠向這些國家提出建設性的建議，同時在向外國軍售時避免採取剝削性策略，這對西方聯盟將是一個機會。在西方制裁破壞國家安全的情況下，西方聯盟如果不提出建設性的建議，可能會嚴重惡化其與幾個強國的關係。

俄羅斯的軍事力量依賴矽生命線——一條從美國經英國、荷蘭、德國、瑞士和法國，再到台灣、韓國和日本的供應鏈生命線。失去了這條生命線，俄羅斯軍隊將注定不得不部署越來越過時的技術，也就失去了其在戰場上的精準和高效。鑑於俄羅斯在常規操作中面對的無法逃避的不利形勢，俄羅斯可能會在軍備方面越來越依賴中國，也可能在衝突中更容易迅速升級到使用戰術核武器。最後，本報告向西方決策者提出如是核心問題：這條矽生命線是否要被切斷，各國又是否為切斷這條生命線所帶來的機會做好了準備。

作者

James Byrne是RUSI的開源情報與分析（OSIA）主任。

Gary Somerville是RUSI OSIA的研究員。

Joseph Byrne是RUSI OSIA的研究員。

Jack Watling是RUSI陸戰高級研究員。

Nick Reynolds是RUSI陸戰研究分析師。

Jane Baker是一名獨立顧問。

RUSI