美军伪冒电子元器件问题现状及对策

胡开博，张 倩，杨志维
（中国工业和信息化部电子科学技术情报研究所，北京 100040）

摘 要：伪冒电子元器件大量进入美军武器装备系统，严重危害美国装备建设和国家安全，引起美国国会、国防部等多部门的高度关注。在美国，伪冒电子元器件大幅增多，致使装备的可靠性降低，加大了装备研制的时间成本和经济成本，并严重威胁网络空间安全。伪冒电子元器件在美国国防供应链中泛滥的主要原因是国防部门监管不力、措施不足。为应对伪冒电子元器件问题，美国政府和军方采取了一系列防范措施，如，制定防止伪冒电子元器件法律条款，开展反伪冒电子元器件技术研发，加大对制售伪冒电子元器件人员的处罚力度等。美国从法律、管理等层面对伪冒电子元器件所采取的应对措施，值得我们参考和借鉴。

关键词：美国；伪冒电子元器件；武器装备；网络空间安全
中图分类号：TN609(712) **文献标识码：**A DOI：10.3772/j.issn.1009-8623.2014.04.005

近年来，武器装备寿命周期（通常 25～30 年）不断增加与电子元器件产品周期（通常 2～5 年）逐渐缩短的矛盾越来越大，大量武器装备面临元器件停产断档或造源萎缩（Diminishing Manufacturing Sources，DMS）的压力，而且电子元器件供应链向全球扩展，这使得军用电子元器件面临巨大的安全可控风险。在美国，伪冒电子元器件大量进入美军武器装备系统，产生了严重影响，引起美国国会、国防部、国土安全部、商务部、国家宇航局、政府问责署等多部门的高度关注。

1 伪冒电子元器件成为武器装备和网络空间安全的重大隐患

综合美国商务部和政府问责署等部门的研究，伪冒电子元器件是指非原厂生产，或者版图及等级、型号、生产日期等信息被更改，意图冒充原厂元器件的伪造品或假冒品[1-6]。伪冒电子元器件大致分为 5 类：非授权的逆向仿制产品、设计或生产环节遭到恶意篡改的产品、旧件翻新产品、不合格件再流通产品及虚假标识产品。2007 年以来，美国政府和军方开展了一系列调查和举证工作，认为伪冒电子元器件问题已对武器装备和网络空间安全带来重大危害。

1.1 伪冒电子元器件大幅增多，殃及众多重要武器装备

（1）伪冒电子元器件案件频发

据美国商务部 2010 年《国防工业基础评估：伪冒电子元器件》[1]报告称，美国国防采办中，伪冒电子元器件案件由 2005 年的 3 369 件增长到 2008 年的 8 644 件，增长了两倍多。尤其近两年，伪冒电子元器件案件呈现更快上升势头。2012 年 2 月，美国知名研究公司 IHS 发布的调查报告[7]进一步显示，2011 年伪冒电子元器件案件数是 2009 年的 4 倍，主要涉及模拟集成电路、微处理器、存储器、可编程逻辑器件和晶体管五大类，并有从集成电路向分立器件扩散的趋势[8]。2012 年 10 月，IHS 公司再次发出警告，伪冒电子元器件案件数仍在以 2011 年的速度继续增长，增

第一作者简介：胡开博（1982—），男，工学硕士，工程师，主要研究方向为基础电子领域科技情报和软科学以及科技创新和战略咨询。
收稿日期：2013-12-29

长率达到 107.3%[9]。

总体来看，美国伪冒电子元器件已渗透到元器件生产商、分销商、装备集成商和国防部等供应链各环节，受影响部门或企业的数量占国防电子供应链的 40%[1]。

（2） 伪冒电子元器件已大量应用于美军现役武器装备

美国政府问责署在 2011 年对国防后勤局、导弹防御局等国防部门和若干装备的调查中，均发现了伪冒电子元器件[4]。2012 年，美国参议院军事委员会调查了 1 800 起伪冒元器件案件，发现进入美军现役装备的伪冒电子元器件数量超过 100 万件，涉及空军 C–17、C–130J、C–27J 运输机和 P–8A 反潜机，海军陆战队 AH–64、SH–60B、CH–46 直升机以及陆军末段高空区域防御系统等[10]。

1.2 伪冒电子元器件显著降低装备可靠性，增加研制时间和成本

伪冒电子元器件在质量可靠性方面存在缺陷，与原厂元器件相比，伪冒电子元器件的性能、可靠性、寿命等通常无法满足军用要求。即使最有可能通过性能检测的翻新器件，根据美国空军的测试，其实际寿命也降至不到原厂器件的 30%[11]。

伪冒电子元器件正成为武器装备性能和可靠性的巨大隐患，即导致武器系统的可靠性每年下降 5%～15%[1]，甚至可使装备失效。例如，美军发现导航系统中的伪冒振荡器将造成无人机无法返回[12]；部署到阿富汗的 2 架 C–27J 运输机中发现的伪冒存储器，使得飞机发动机状态、燃料情况、诊断数据等重要信息极易丢失[10]。在战时等极端严酷环境下，伪冒元器件甚至会直接导致装备失效，如，2009 年美军“捕食者”无人机在阿富汗对重要目标人物发动攻击的一刻突然坠毁，原因正来自飞控系统中的伪冒元器件。该事件致使美国国防部停飞所有该型无人机，以接受检查。[13]

伪冒电子元器件一旦装机，其检验、替换的时间成本与经济成本将十分巨大。仅替换现役装备中仿制和翻新的电子元器件的费用就将高达数亿美元[14]，即使单型装备中伪冒电子元器件的替换成本也极为高昂，如，陆军末段高空区域防御系统中伪冒电子元器件的替换费用预计为 270 万美元[10]。同时，伪冒电子元器件也成为导致装备研制项目超期或超支的重要原因之一，美国国家宇航局某探测项目曾因此不得不延期 9 个月，并超支 20%[15]。

1.3 被恶意篡改的元器件严重威胁网络空间安全

微处理器是网络空间的重要构成，一旦被植入恶意电路，可导致其性能劣化、功能失效，信息被窃取或被监听控制等。即使不更改电路，仅在生产过程中对参数做出细微修改，也可显著降低器件的可靠性。目前，美国已掌握恶意电路植入技术，并验证了人为工艺缺陷，可使设计寿命 15 年的军用卫星在 6 个月后失效[16]。

美国军用集成电路 90% 以上依赖海外制造，国防科学委员会、导弹防御局、联邦调查局和国土安全部等多个国防和政府机构均表示，集成电路可能在设计或生产环节遭恶意篡改，危害美国网络空间安全，并称，已发现有销往美国的商用元器件被预置了恶意电路[17-19]。《国防部网络空间行动战略》[21] 作为美军网络空间发展的纲领性文件，强调电子元器件供应链的安全，并将信息产品中可能被植入恶意电路确定为重大威胁。

2 监管不力、措施不足是美国伪冒电子元器件问题日益严峻的主要原因

受利益驱使制售伪冒电子元器件活动日益猖獗，而且在流通、采购、检验、供应商管理等环节缺乏有力监管和应对措施，导致伪冒电子元器件在美国国防系统中蔓延和泛滥。

2.1 缺乏对伪冒电子元器件有效监管和处置措施

综合美国多个部门的调查，国防部门对伪冒电子元器件的监管和处置存在以下薄弱环节：

（1） 国防部对伪冒电子元器件尚无统一定义，对已发现的伪冒电子元器件也没有明确的处置要求，导致各方针对伪冒电子元器件的相关工作缺少统一的认识和工作基础；

（2） 规范国防采购的《国防联邦采购法》未制定防止伪冒电子元器件的专门条款，使得相关工作缺少权威、有效的法律依据；

（3） 国防部和其他政府机构对列入国防供应商名录中企业的产品和资格复核不及时，以致获得认证的分销商却成为伪冒电子元器件的最大来源；

（4） 包括负责国防部采购的国防后勤局等在内的众多国防部门，在电子元器件的采购、检测、

废件处理等环节尚未建立有效的应对措施，以致调查中出现已被国防部门判定为不合格的产品再次进入国防供应链的情况；

（5）已有规避手段没有发挥实效，一是关于伪冒电子元器件的标准未得到有效实施，仅有的国家宇航局制定的 AS5553 标准——《伪冒电子元器件参考而未强制实行[3, 21]；二是国防部两大数据库“产品数据报告和评估项目”和“共同缺陷报告系统”对伪冒元器件的监控基本没有发挥实际意义；三是国防部和国家宇航局拥有先进的检验设施和严格的检验标准，但对交付装备中的元器件并未进行任何检测。

2.2 分销商和互联网成为伪冒电子元器件的最大来源和流通平台

独立分销商通常可为用户提供较好的供货周期、价格及停产断档产品，是军用电子元器件供应链中不可或缺的重要环节，然而，由于缺少检测设施和政府监管以及对灰色市场的依赖，独立分销商受利益驱使制售伪冒电子元器件，已成为伪冒电子元器件的最大来源。值得注意的是，由于电子元器件生产商的废件处理、产品退货、分销商授权与问责等管理制度不完善，即使信任度较高的生产商和授权分销商的产品中也存在伪冒电子元器件。

另外，由于缺少监管，作为军方停产断档元器件重要交易市场的互联网，已成为伪冒电子元器件制售者偏好的供销平台，甚至一些大型电子元器件网络供销商因疏于对供应商的资质考核，沦为了伪冒电子元器件的集散地。美国政府问责署于 2012 年 2 月发布《国防部供应链：互联网采购平台供应疑似伪冒元器件》[22] 报告，进一步说明了互联网交易平台上伪冒电子元器件泛滥的严重性。

2.3 装备集成商缺乏防范措施，采购并使用了伪冒电子元器件

装备集成商及子系统集成商尚未建立完备的伪冒电子元器件防范措施，雷声、L–3 通信、波音等众多装备集成商均在不知情的情况下使用了伪冒电子元器件，其原因主要有 3 个方面：一是采购中缺乏监管，迫于停产断档或价格、货期的压力，存在采购人员擅自从独立分销商采购元器件的现象[12]；二是缺少有效检测手段和入检标准，而且制售伪冒电子元器件的技术和手段不断改进，如，有的销售商通过采购与原厂元器件相同的外壳和打标设备，将伪冒元器件与原厂元器件混杂销售，使得镜检和抽样检查等常规检查手段难以奏效；三是对能够提供停产断档产品的上游供应商缺少相应的产品质量评价体系，合同中也无规避伪冒元器件的条款，导致伪冒电子元器件通过一级一级的子承包商最终进入装备集成商。

3 多部门共同应对伪冒电子元器件问题

为应对日益严峻的伪冒电子元器件问题，美国政府和军方自 2011 年至今采取了一系列积极的应对措施。

3.1 制定防止伪冒电子元器件法律条款

美国国防部在《2012 财年国防授权法》[23] 中，首次制定了针对伪冒电子元器件的条款。该法案规定：立即评估国防部现有采购政策及对伪冒电子元器件的防范能力；必须制定统一的“伪冒电子元器件”定义，并发布具体的防范指南；修订《国防联邦采购法》，增加防范伪冒电子元器件的相关条款。国家宇航局也在此前《国家宇航局授权法》[24] 中新增了类似内容。此外，法案特别强调加强对装备集成商及电子元器件供应商的管理，主要包括：改进国防部和国家宇航局对元器件供应商的认证和考核，增加技术和管理等具体要求，提高准入门槛，按需分级建立可信供应商名录并定期考核和调整；装备集成商必须从可信或许可的供应商采购电子元器件，并制定采购、检验、人员培训、跟踪与上报等具体策略，同时，对上游子供应商提出同样要求；如果在装备中发现伪冒电子元器件，维修替换工作及其费用全部由装备集成商负责，国防部有权立即终止合同并拒付任何费用。

应法案要求，美国国防部负责采办、技术与后勤（AT&L）的副部长以及国防后勤局、国防联邦采购管理委员会在 2012 年采取了多项应对措施。2012 年 3 月，美国国防部发布“国防部防范伪冒电子元器件最高指南”备忘录[25]，对伪冒做出定义，并给出具体防范、检测方法和补救措施；同年 12 月，国防后勤局启动“通过测试认证的供应商名录”项目[26–27]，拟通过预先审核方式建立关键、停产的元器件供应商名单。2013 年 5 月，《国防联邦采购法》中新增 2012–D055“伪冒电子元器件的

检测和防范”条款[28]，对伪冒电子元器件定义、装备集成商责任、政府职能等内容做出明确规定。目前，该条款已通过美国国防采办管理委员会的审核，处于最终修订阶段。

3.2 开展反伪冒电子元器件技术研发

美国国防部门加大元器件防篡改、伪冒元器件鉴别和恶意芯片检测三大技术的研究力度。国防先期研究计划局于 2007 年和 2010 年启动“可信集成电路”、“完整可靠集成电路”项目[29–30]，大力发展恶意芯片检测技术，确保元器件尤其是集成电路产品安全可用。2011 年，美国海军实施“电子系统保护”项目[31–32]并研制出物理不可复制功能（PUF）技术[33]。该技术已应用在美国美高森美公司 2012 年 10 月推出的具有最高安全特性的现场可编程门阵列产品中，以期从根源上防止元器件被逆向仿制。此外，2012 年初，国防后勤局研制出可用于元器件防伪标识的植物 DNA 技术。受国防部委托，爱达荷国家实验室证实该技术无法破解和仿造，可有效防伪；2012 年 8 月，国防后勤局在国防后勤采办指令 52.211–9 074 中新增“高危器件使用 DNA 标识”条款[34]，要求“联邦供应目录——微电子电路”中的供应商为其供应的产品从 2012 年 11 月起必须带有植物 DNA 防伪标识。但由于成本等原因，目前该要求实施缓慢。

3.3 加大处罚力度，加强电子元器件进出口管理

美国多部门协同，不断加大伪冒电子元器件案件查处力度。司法部牵头专门成立了“伪冒微电子器件工作小组”[35]，对制售伪冒电子元器件的人员进行调查和起诉，司法部联合国土安全调查办公室、海军罪案调查处等部门至少刑拘了 5 家向军方销售伪冒电子元器件公司的负责人。另外，国会对《伪冒商品交易法案》进行了修订，将制售伪冒电子元器件的个人和公司的处罚金额分别提高至 200 万和 500 万美元，人员监禁上限由 5 年提高到终身监禁[36]。在电子元器件进出口管理方面，海关与边境保护局已表示，将加大对伪冒电子元器件入关时的关检力度；国土安全部正研究建立发现进口产品中伪冒电子元器件的评估体系。

4 启示

军用电子元器件在建设信息化武器装备中发挥着至关重要的基础性作用，其质量可靠性一旦出现大面积的问题，将侵蚀一个国家武器装备性能和可靠性的根基。美国是武器装备研建大国，同时又是军用电子元器件技术最先进的国家，伪冒电子元器件却日益泛滥，其影响如此之大、管控如此之难，值得其他国家高度警觉。

（1）高度重视伪冒电子元器件问题

伪冒电子元器件虽在 2007 年就引起美国海军注意，但并未受到国防部和装备集成商的足够重视，近两年，大量出现并对装备建设造成了严重影响。虽然美军制定了一系列防范措施，但目前来看，部分实施效果并不理想，如，相关法规和国防指令的修改远落后于国防部的时间要求，采用 DNA 标识的元器件供应商至今（2013 年 12 月）也只有 26 家。为此，我国应引以为鉴，尤其是目前我军正处于信息化建设的关键时期，更应树立起对伪冒电子元器件问题的重视，将其视为我军装备建设的重大问题予以看待，及时开展调查，摸清我军装备建设中伪冒电子元器件的影响和根源，提早发现问题并做出研判。

（2）主动应对伪冒电子元器件技术风险

至今未有明确证据显示美国遭遇恶意芯片的案例，而且美国集成电路技术水平遥遥领先，却大力投资研发防御技术，硬件木马易攻难防，因此，相关技术很有可能转化为攻击手段。此外，芯片内互联线上的人为工艺缺陷可导致芯片过早失效，该方式更加易用、更加隐蔽。我国军用电子元器件采购渠道复杂，更加依赖分销商，自主设计的关键产品也依赖外资或合资工艺线制造，其中的风险不容小觑。我国应尽快开展伪冒电子元器件检测技术研究，重点研究恶意芯片检测技术和元器件防篡改技术，确保进口或外资线制造的电子元器件安全可靠。

（3）大力加强军用电子元器件供应链监管

美国从法律、管理等层面对伪冒电子元器件问题所采取的具体应对措施，值得我们参考和借鉴。与美国相比，由于装备建设的内、外部环境不同，我军伪冒电子元器件问题必将有着不同的原因和特点。应尽快研究在采办法规中加入防范伪冒电子元器件的条款，制定相关标准，并逐步推广施行；加强对元器件各级供应商的资质考核和动态管理，提出防范伪冒电子元器件的具体要求，同时特别要强

化整机单位和系统集成单位的主体责任；军方、工业、司法等多部门联合协同，加大对制售伪冒电子元器件的检查、追责和处罚力度。■

参考文献：

[1] U.S. Department of Commerce.Defense Industrial Base Assessment: Counterfeit Electronics[R]. Washington, DC: Department of Commerce Bureau of Industry and Security Office of Technology Evaluation, 2010-01.

[2] Hughitt B. Counterfeit Electronic Parts[R]. Washington, DC: NASA/ESA/JAXA Trilateral Safety and Mission Assurance Conference, 2008-04.

[3] Hughitt B. Counterfeit Electronic Parts[R]. Washington, DC: NEPP Electronics Technology Workshop, 2010-06.

[4] Hillman R J. DoD Supply Chain: Preliminary Observations Indicate That Counterfeit Electronic Parts Can Be Found on Internet Purchasing Platforms[R]. Washington, DC: Government Accountability Office, 2011-11.

[5] Counterfeit Parts: Increasing Awareness and Developing Countermeasures[R]. Arlington, Virginia: Aerospace Industries Association of America, 2011-03.

[6] AS5553: Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition[S]. Washington, DC: SAE International, 2009-04.

[7] Reports of Counterfeit Parts Quadruple Since 2009, Challenging US Defense Industry and National Security[R]. Englewood, Colorado: IHS iSuppli Corporation, 2012-02.

[8] IHS iSuppli Corporation. Top 5 Most Counterfeited Parts Represent a $169 Billion Potential Challenge for Global Semiconductor Market[EB/OL].(2012-04-04)[2013-12-26]. http://www.isupplicom/Semiconductor-Value-Chain/News/pages/Top-5-Most-Counterfeited-Parts-Represent-a-$169-Billion-Potential-Challenge-for-Global-Semiconductor-Market.aspx.

[9] IHS iSuppli Corporation. Electronic Component Counterfeit Incidents Continue Record Pace[EB/OL].(2012-10-2)[2013-12-26]. http://www.isuppli.com/semiconductor-value-chain/news/pages/electronic-component-counterfeit-incidents-continue-record-pace.aspx.

[10] Levin C, McCain J. Senate Armed Services Committee Releases Report on Counterfeit Electronic Parts[R]. Washington, DC: Senate Committee On Armed Services, 2012-05.

[11] Fake Parts are Seeping Into Military Aircraft Maintenance Depots[R]. Museum, Ohio: Air Force, 2008-03.

[12] Defense Supplier Base: DoD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts[R]. Washington, DC: Government Accountability Office, 2010-03.

[13] The Industrial College of the Armed Forces. Electronics Industry Final Report[R]. Washington, DC: National Defense University, 2010-05.

[14] Levin C. Opening Statement at SASC Hearing on Counterfeit Electronic Parts in DOD Supply Chain[EB/OL].(2011-11-08)[2013-12-26]. http://www.levin.senate.gov/newsroom/speeches/speech/opening-statement-at-sasc-hearing-on-counterfeit-electronic-parts-in-dod-supply-chain.

[15] PR Newswire Corpration. NASA's Anti-Counterfeiting Measures Fall Short of Validating Parts Authenticity[EB/OL].(2010-05-06)[2013-12-26]. http://www.prnewswire.com/news-releases/nasas-anti-counterfeiting-measures-fall-short-of-validating-parts-authenticity-92955159.html.

[16] Adee S. The Hunt for the Kill Switch[J]. IEEE Spectrum, 2008, 45(5): 34–39.

[17] High Performance Microchip Supply[R]. Washington, DC: U.S. Defense Science Board, 2005-02.

[18] Buying Commercial: Gaining the Cost/Schedule Benefits for Defense Systems[R]. Washington, DC: U.S. Defense Science Board, 2009-02.

[19] Snow G M. Statement Before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism[EB/OL].(2011-04-12)[2013-12-26]. http://www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism.

[20] Department of Defense Strategy for Operating in Cyberspace[R]. Washington, DC: U.S. Department of Defense, 2011-07.

[21] Zulueta P. Counterfeit Electronics NASA Update[R]. Washington, DC: Jet Propulsion Laboratory, National Aeronautics and Space Administration, 2011-06.

[22] US Government Accountability Office. DoD Supply Chain: Suspect Counterfeit Electronic Parts Can Be Found on Internet

Purchasing Platforms[R]. Washington, DC: GAO, 2012-02.

[23] National Defense Authorization Act for Fiscal Year 2012 [S]. Washington, DC: 112th Congress, 2011-12.

[24] National Aeronautics and Space Administration Authorization Act of 2010[S]. Washington, DC: 111th Congress, 2010-10.

[25] U.S. Department of Defense. Overarching DoD Counterfeit Prevention Guidance[R]. Washington, DC: The Under Secretary of Defense, 2012-03.

[26] Defense Logistics Agency. Qualified Testing Suppliers List[EB/OL]. (2012-12-27)[2013-12-26]. http://www.dla.mil/InformationOperations/sirc/Lists/News%20Feed/CustomDispForm.aspx?ID=50.

[27] Qualified Testing Suppliers List (QTSL), Qualification Notice, FSC 5961 and 5962[R]. Fort Belvoir, Virginia: Defense Logistics Agency, 2013-06.

[28] U.S. Department of Defense. Defense Federal Acquisition Regulation Supplement: Detection and Avoidance of Counterfeit Electronic Parts (DFARS Case 2012-D055) [S]. Washington, DC: Defense Acquisition Regulations System, Department of Defense, 2013-05.

[29] Colwell R. Trusted Integrated Circuits (Trust)[EB/OL]. [2012-12-20]. http://www.darpa.mil/Our_Work/MTO/Programs/Trusted_Integrated_Circuits_(TRUST).aspx.

[30] Bernstein K. Integrity and Reliability of Integrated Circuits (IRIS)[EB/OL]. [2012-12-20]. http://www.darpa.mil/Our_Work/MTO/Programs/Integrity_and_Reliability_of_Integrated_Circuits_(IRIS). aspx.

[31] Keller J. Advanced Anti-Tamper Technologies Are Goal of Navy Protection of Electronics Systems Solicitation [EBOL]. (2011-04-21)[2013-12-26]. http://www.militaryaerospace.com/articles/2011/04/advanced-anti-tamper.html.

[32] U.S. Navy. Protection of Electronics Systems[R]. Arlington, Virginia: Office of Naval Research, 2011-04.

[33] Love E, Jiny Y, Makris Y. Enhancing Securityvia Provably Trustworthy Hardware in Intellectual Property[C]// 2011 IEEE International Symposium on Hardware-Oriented Security and Trust. San Diego, California, 5-6 June 2011. San Diego, CA: IEEE,2011-06: 12-17.

[34] Defense Logistic Acquisition Directive 52. 211–9074[S]. Washington, DC: Department of Defense, 2012-11.

[35] U.S. Department of Justice. U.S. Attorney's Office for the District of Columbia Leads Effort to Combat Counterfeit Microchips[EB/OL]. [2013-12-26]. http://www.justice.gov/usao/briefing_room/cc/mca_cyber_crime.html.

[36] 18 U.S. Code 2320–Trafficking in Counterfeit Goods or Services[S/OL]. [2013-12-26]. http://www.law.cornell.edu/uscode/text/18/2320.

Issue of Counterfeit Electronic Component in the United States and Its Countermeasures

HU Kai-bo, ZHANG Qian, YANG Zhi-wei

(Electronic Technology Information Research Institute, Ministry of Industry and Information Technology of the People's Republic of China, Beijing 100040)

Abstract: Counterfeit electronic components have flushed into the U.S. military weapon equipment systems in great quantities, causing serious damage to the weapon construction and national security, and drew heightened concern of the U.S. congress, the department of Defense (DoD), the Department of Homeland Security (DHS) and so on. This paper studied the concept and scope of counterfeit electronic components, as well as their influence on weapon systems and cyberspace security in the U.S., analyzed the main reasons why counterfeit electronic components invaded the defense supply chain, and generalized a series of preventing measures taken by

(下转第 66 页)

1989(5)：32–33.

[8] Forge S, Blackman C, Goldberg I, et al. Comparing Innovation Performance in the EU and the USA: Lessons from Three ICT Sub-Sectors[R]. Seville, Spain: Joint Research Centre of the European Commission, 2013: 90.

[9] 网易公开课. 罗德尼·布鲁克斯: 我们为什么要找机器人帮忙？[DB/OL]. [2014-01-08]. http://v.163.com/movie/2013/11/9/5/M9C2SL6Q2_M9C2SRV95.html.

[10] 谢勒 F M. 产业结构、战略与公共政策[M]. 张东辉等译. 北京：经济科学出版社，2010–07–02.

Innovation of U.S. Service Robot Industry : Experience and Lessons from iRobot

WANG Ying-chun, SHEN Ying-long

(Shanghai Institute for Science of Science, Shanghai 200235)

Abstract: The U.S. company iRobot is a global leader in developing service robots. It has applied robots technologies towards commercial and civil use successfully owing to its good entrepreneurial environment, sophisticated achievement transfer system, and strong technology accumulation. On the other hand, supports from the government ensure survival and development of iRobot. The paper highlights the development and experience of iRobot, and analyzes features and supporting conditions of innovation of U.S. service robot industry, and gives some insights as follows: The development of emerging technology industry with long-time high uncertainty is a very complex process. It needs effective integration of resources from government, enterprises and research institutes. The government should provide a dual-support from both the R&D investment and market demands to push the integration of advanced technology and the practical needs. For the enterprises, choosing right breakthrough points of product ideas and market share is the most important.

Key words: United States; iRobot; service robots; industrial innovation

Issue of Counterfeit Electronic Component in the United States and Its Countermeasures

HU Kai-bo, ZHANG Qian, YANG Zhi-wei

(Electronic Technology Information Research Institute, the Ministry of Industry and Information Technology of the People's Republic of China, Beijing 100040)

(上接第 26 页) the U.S. government and military, such as establishing legal system to guard against counterfeit electronic components, supporting technologies of anti-counterfeit electronic components, imposing punishment to offenders involved in manufacturing counterfeit electronic components, which is worthwhile to be shared by Chinese counterparts.

Key words: the U.S.; counterfeit electronic component; weapon and equipment; cyberspace security