

普京首轮出访昭示俄外交走向



5月31日至6月7日，新任俄罗斯总统普京将进行首轮密集出访。所访问的国家中既有白俄罗斯、哈萨克斯坦、乌兹别克斯坦及中国这样的传统友好国家，也有德国和法国这样西方国家。

观察家认为，从普京这次即将出访的国家来看，俄罗斯今后仍将奉行东西方平衡的外交政策，继续深化中俄战略协作伙伴关系，强化与独联体国家关系，推动独联体国家小范围一体化将成为俄外交政策的优先方向。

美欧“待遇”不同

普京当选总统后，有国际舆论猜测俄罗斯与西方国家的关系将变冷，俄外交政策重心将转向东方。实际上，苏联解体后，俄罗斯大部分时间都奉行东西方平衡的外交政策。从此次普京首轮出访看，在西方国家中，俄将重点发展与德、法等友好国家的关系。

有分析指出，尽管发展俄美关系历来在俄外交中占有优先地位，但美国无视俄在反导系统问题上的关切，单方面推动欧洲反导系统的部署，加上双方在短期内达成妥协的可能性很小，俄已做好两国关系降温的准备。

最近一系列事件已显露出俄美

关系降温的某些征兆：先是美国对普京当选总统“不冷不热”，接着普京以“忙于组阁”为由没有出席在美国举行的八国峰会。而美国总统奥巴马也“以牙还牙”，以竞选为由表示将不会出席今年在俄罗斯举行的亚太经合组织峰会。

在俄美关系微妙变化的同时，普京不仅选择德、法为首轮出访的西方国家，还将出席在圣彼得堡举行的俄罗斯—欧盟峰会，这足以说明普京对发展俄罗斯与德法两国以及与欧洲关系的期待和重视。

普京之所以在西方国家中如此重视德法两国，首先是因为欧盟，尤其是德国是俄主要经贸伙伴，俄非常

担心欧债危机影响欧盟经济发展。欧盟经济发展前景将是普京出访德法两国的重要议题。

其次，俄与德法两国领导人向来私交很好，两国在许多重大问题上曾支持俄罗斯。而前不久法国领导人更替增加了法俄关系的不确定性，普京访法旨在了解法国新领导人对俄政策的基调。

第三，德法两国是欧盟国家中的经济和政治大国。俄罗斯同西方在叙利亚问题、伊朗核问题、欧洲反导问题以及中亚驻军等诸多问题上存在分歧。有舆论认为，俄罗斯希望通过强化与德法等国关系来分化美欧，以在上述问题上缓解来自西方的压力。

独联体国家优先

在普京总统首轮出访的6个国家中，独联体国家就有3个，而且白俄罗斯还是普京首个出访国。这足以说明独联体国家在俄外交中的重要性。

近年来，俄罗斯积极推动与白俄罗斯和哈萨克斯坦两国的一体化进程。按计划，三国将在2015年建立欧亚经济联盟，届时将实现资金、人员和货物的自由流动。白、哈两国是俄

当局推动独联体一体化的主要支持者、参与者和重要依托，它们在俄罗斯外交中的重要性不言而喻。

早在俄总统选举前，普京就一再强调发展俄罗斯与独联体国家关系、推动独联体一体化的重要性。专家认为，强化与独联体国家关系、推动与白哈等独联体国家之间的小范围一体化以及建立欧亚经济联盟将成为普京本届总统任期的优先任务。

普京此次出访乌兹别克斯坦也有其考量。最近几年，乌兹别克斯坦与俄罗斯若即若离，对俄推动的独联体一体化进程保持警惕。从去年开始，俄乌关系开始升温，乌兹别克斯坦比以往更积极地参与独联体的活动。这说明俄在独联体国家扩大影响力取得成效，普京希望通过访乌进一步拉近两国关系，增强俄在独联体国家的影响力。



资料图：普京

深化对华关系

对发展俄中关系高度重视。

普京3月初当选俄总统后，中国国务院副总理李克强就在4月底访问俄罗斯，与俄政府、议会领导人举行了会晤，同俄工商界进行了广泛接触，就进一步深化中俄战略协作伙伴关系达成共识。时过一个月，新任总统普京又将访问中国。

分析人士认为，两国领导人互访如此频繁，这在国家间关系中并不多见，且这次首轮出访普京将在中国停留时间最长。这充分说明发展与中国关系在俄外交政策中的分量。

(据新华社电)

最复杂电脑病毒“火焰”曝光

该病毒具有强大的间谍功能 窃取资料后即神秘消失



俄罗斯电脑病毒防控机构卡巴斯基实验室28日发布报告，确认新型电脑病毒“火焰”入侵伊朗等多个中东国家。病毒用于窃取信息，部分特征与先前攻击伊朗核设施电脑系统的Stuxnet蠕虫病毒相似，但结构更复杂、损害更大。技术人员以“网络攻击武器”定性“火焰”，推测这一病毒可能有政府背景。专家称这种病毒很可能是已发现的最复杂恶意程序之一。

病毒程序构造复杂前所未有



伊朗核设施内的计算机系统曾多次遭到电脑病毒攻击，一些用于铀浓缩的离心机因此无法运行。

目前，研究人员还不清楚这种蠕虫病毒(Worm.Win32.Flame)最早是如何进入电脑系统的。不过，卡巴斯基实验室最早在一些联合国下属机构(International Telecommunication Union)电脑中发现了该病毒的踪迹。当时，该组织发现，来自中东地区的敏感文件莫名其妙丢失。

专家介绍说，这种新型病毒最重要的应用是它的间谍功能。感染该病毒的电脑将自动分析使用者的上网规律，记录用户名密码，自动截屏并保存一些文件和通讯信息，甚至可以暗中打开麦

克风进行秘密录音等，然后再将窃取到的这些资料发送给远程操控该病毒的服务器。

“火焰”之所以拥有如此强大的间谍功能，是因为它的程序构造十分复杂，“火焰”所包含的代码数量相当于之前发现的“震网”病毒(Stuxnet)或“毒区”病毒(Duqu)的20倍，此前从未有病毒能达到这种水平。它可以通过USB存储器以及互联网进行复制和传播，并能接受来自世界各地多个服务器的指令。一旦完成搜集数据任务，这些病毒还可自行毁灭，不留踪迹。

已入侵伊朗等多个中东国家

虽然这种病毒是在最近才被发现的，但很多专家认为它可能已经存在了5年之久，包括伊朗、以色列、黎巴嫩、沙特和埃及在内的成千上万台电脑都已感染了这种病毒。而且这种病毒的攻击活动不具规律性，个人电脑、教育机构、各类民间组织和国家机关都曾被其光顾过。电子邮件、文件、消息、内部讨论等等都是其搜集的对象。

伊朗全国电脑紧急状况应对小组证实发现这种病毒。这一机构在它的英文网站发布消息，说“火焰”可能

关联伊朗数起电脑系统信息失窃事件。

“火焰”被曝光以后，伊朗已经决定对该国所有官方机构的电脑系统进行紧急检查，以便排除可能受到的病毒袭击。

俄罗斯著名电脑安全公司卡巴斯基高级研究员罗埃尔·斯考文伯格表示：“如果‘火焰’病毒真的已经存在了5年而没被发觉，那么唯一合乎逻辑的结论是，肯定还有其他正在进行的网络攻击，只是我们尚未发现而已。”

以色列高官暗示与病毒有关

以色列分管战略事务的副总理摩西·亚阿隆29日说，以“火焰”等电脑病毒发起攻击等方式阻止伊朗核活动的做法“合理”。

亚阿隆告诉以色列军方电台，“对于任何视伊朗有重大威胁的人，采取不同措施以牵制伊朗的做法合理，包括那些(措施)”，即指以电脑病毒攻击伊朗。他说，以色列技术资源“丰富”，“那些工具(电脑病毒)为我们开放各种可能”。

以色列和美国等一些国家指认伊朗秘密研制核武器，伊朗方面坚称自己的核计划出于民用目的。

在此之前，伊朗核设施内的计算机系统曾多次遭到“震网”和“毒区”的攻击，一些用于铀浓缩的离心机因此无法运行。伊朗石油部门网络系统也曾遭某种电脑病毒袭击，最大原油出口基地立即断网防止病毒扩散，原油出口未受影响。

(据《钱江晚报》)