大众安全威胁感知钝化研究*

齐桐萱

【内容提要】 当安全威胁长期存在时，大众威胁感知有时会随着威胁发展而同步上升，有时其大小或增速衰减，出现安全威胁感知钝化现象。那么，大众安全威胁感知钝化出现的条件及其发生机制为何？本文认为，安全威胁事件可以分为两种类型，分别是新生威胁事件和重复威胁事件。在新生威胁事件下大众安全威胁感知不钝化，而在重复威胁事件下，大众安全威胁感知则钝化。安全威胁感知钝化出现的机制在于，随着安全威胁事件的不断发生，人们关于安全威胁的信息增加、知识增长，熟悉性上升，关于安全威胁的不确定性下降，因而恐惧感降低，从而出现钝化现象。通过美意大众对网络攻击威胁感知的变化以及法国大众对恐怖主义威胁感知变化的案例分析，本文对假设进行了检验。本文的研究发现说明，长时间积累下的信息、知识和熟悉性能够改变大众对威胁的恐惧心理，并影响威胁感知大小。它们的作用在短时间内也许难以察觉，但长期累积最终会显现其影响。在对安全威胁感知的研究中，应当重视时间因素的作用。

【关键词】 安全威胁　安全认知　大众威胁感　时间因素

【作者简介】 齐桐萱，北京外国语大学亚洲学院讲师。
电子邮箱：qitx@bfsu.edu.cn

* 本文系国家社会科学基金重大项目“新时代下国际领导力研究”（项目批准号：21&ZD167）的阶段性成果。感谢《国际政治科学》匿名评审专家及编辑部的宝贵意见和建议，文中错漏由笔者负责。

一、问题的提出

1947 年，美国《原子科学家公报》创建“末日时钟”，这是用来表达核威胁引发“世界末日”所剩余时间的虚拟时钟。当世界上发生严重核威胁事件时，末日时钟会向前拨动，表示人类距离“世界末日”更近。① 这表明，当核威胁增长时，人们相应的安全威胁感知也随之增大。然而，威胁及其感知的关系并不总是正相关的，有些时候，虽然安全威胁在发展，但大众的安全威胁感知却在下降。例如，根据相关网络攻击数据库的数据统计，西班牙 2017 年网络攻击事件总数量是 2016 年总数量的三倍多，②但认为网络攻击威胁是国家所面临主要安全威胁的西班牙民众比例在 2016 年是 67%，在 2017 年却下降至 65%。③ 再如，2002 年至 2008 年，美国境内因恐怖主义袭击所造成的死亡总人数为 7 人，从 2009 年到 2014 年死亡总人数则为 82 人。④ 然而，相关研究显示，从 2002 年到 2008 年，认为恐怖主义威胁是当前所面临最严重问题的美国民众比例的总体平均水平明显高于 2009 年至 2014 年。⑤

可见，对于安全威胁的变化，大众在感知上有时会出现迟钝化和非敏感

---

① Bulletin of the Atomic Scientists, https://thebulletin.org/doomsday-clock，访问时间：2024 年 6 月 2 日。

② 数据结果根据以下网络攻击数据库数据加总计算得出：CISSM Cyber Attacks Database, University of Maryland, https://cissm.umd.edu/cyber-events-database, 访问时间：2024 年 11 月 5 日；Nancy Gallagher and Charles Harry, “Classifying Cyber Events,” *Journal of Information Warfare*, Vol. 17, No. 3, 2018, pp. 17-31.

③ Jacob Poushter, Moria Fagan and Sneha Gubbala, “Climate Change Remains Top Global Threat Across 19-Country Survey,” Pew Research Center, August 31, 2022, https://www.pewresearch.org/global/2022/08/31/climate-change-remains-top-global-threat-across-19-country-survey/, 访问时间：2023 年 4 月 28 日。

④ Erin Miller, “American Deaths in Terrorist Attacks, 1995—2019,” https://www.start.umd.edu/pubs/START_AmericanTerrorismDeaths_FactSheet_Oct2020.pdf, 访问时间：2024 年 10 月 27 日。

⑤ John Mueller and Mark G. Stewart, “American Public Opinion on Terrorism since 9/11: Trends and Puzzles,” March, 2016, https://politicalscience.osu.edu/faculty/jmueller/tpoISA16.pdf，访问时间：2024 年 10 月 27 日。

化,低估安全威胁的危害性,即“钝化”现象。但另一方面,这种钝化现象也并非一直存在。那么,大众安全威胁感知钝化现象出现的条件及机制是什么?这便是本文的研究问题。

大众安全威胁感知是国际关系研究的重要概念之一,也经常被应用于外交政策分析等研究中。已有相关研究普遍关注于某个时间点上大众安全威胁感知的影响因素,是一种“快照”式的研究,而非长时段研究。对于大众安全威胁感知长时期内如何发展变化,当前文献普遍缺少分析,也并不能很好地说明钝化现象发生的机制。可见,一方面大众安全威胁感知被广泛用于研究分析,但另一方面,对其变化发展规律,当前仍缺少深入的认识。在缺乏对大众安全威胁感知变化规律充分认识的情况下,贸然使用这一概念研究其他问题,很可能导致谬误。因此,对于大众安全威胁感知钝化现象的研究具有必要性。在之后的行文中,本文将首先回顾既有关于大众安全威胁感知影响因素的研究,然后进一步分析时间因素如何影响大众威胁感知变化,阐述大众安全威胁感知钝化发生的条件及机制。在此之后,将以美国和意大利网络攻击威胁下大众安全威胁感知变化,以及法国民众对于恐怖主义威胁的感知变化为案例进行假设检验,最后对本文进行总结。

二、大众安全威胁感知既有文献及不足

已有文献总体上从四个视角分析大众安全威胁感知变化,分别是客观来源、依赖条件、社会建构和心理建构角度。这四类文献可以分别归属于两个大的类别,即影响威胁感知的客观因素和主观因素。第一个和第二个类别的解释属于客观因素分析,而第三和第四个类别的文献属于主观因素分析。

(一)安全威胁感知的外部客观来源

客观威胁大小影响安全威胁感知,这既适用于解释领导人和精英感知变化,也适合于解释大众的感知变化。这类解释强调外部威胁本身对于威胁感知的基础影响作用,认为客观威胁越大,威胁感知水平越高。在这种逻辑下,持有这类视角的学者进一步分析客观威胁来源因素如何影响了威胁

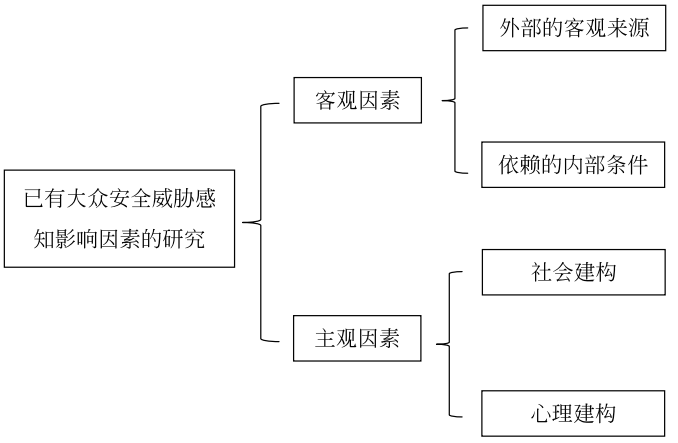

图 1 大众安全威胁感知已有研究梳理总结

来源:作者自制。

感知。如大卫·辛格尔(David Singer)认为,“威胁感知来自武装敌对的情境”。① 再如,斯蒂芬·沃尔特(Stephen M. Walt)在《联盟的起源》中提出了四种影响威胁水平的因素,即综合实力、地缘的邻近性、进攻实力和侵略意图。他认为,地理位置越相近,综合国力越强,进攻实力越强,威胁水平越高。② 除了军事实力、进攻实力以及综合实力等因素,学者们还发现了敌国同盟关系、军事实力的不同要素、国际环境带来的威胁来源变化等因素对威胁感知的影响作用。③

客观威胁本身确实对威胁感知发挥着基础性的作用。然而,客观威胁

---

① J. David Singer, “Threat-Perception and the Armament-Tension Dilemma,” *The Journal of Conflict Resolution*, Vol. 2, No. 1, 1958, p. 94.

② Stephen M. Walt, *The Origins of Alliance*, New York: Cornell University Press, 1987, pp. 22-26.

③ Tomonori Sasaki, “China Eyes the Japanese Military: China's Threat Perception of Japan since the 1980s,” *The China Quarterly*, *2010*, Vol. 203, pp. 560-580; Lora Saalman, “Divergence, Similarity and Symmetry in Sinoi-Indianthreat Perceptions,” *Journal of International Affairs*, Vol. 64, No. 2, 2011, pp. 169-194; 刘雪林:《冷战后日本国家安全观的形成——基于对“威胁”的认知和价值性判断》,载《东北亚学刊》,2017年第1期,第23—28页。

大小对于安全威胁感知的解释力是有限的,如前文所举美国恐怖主义威胁和西班牙网络攻击威胁的案例。两个案例中,客观威胁均有所增长,但大众威胁感知却都出现了下降。因此,除了客观威胁水平之外,应当探究其他能够影响大众威胁感知的因素。

(二)安全威胁感知依赖的内部条件

在客观威胁水平这一因素之外,学者们也发现了安全威胁感知依赖的内在条件,主要包括文化、历史和政治因素等。相似文化能够产生更低的威胁感知,而异质文化则可能产生更高的威胁感知。如有针对美国民众的研究发现,他们抱有敌意的国家均为非西方国家,文化因素影响了他们的威胁感知。① 历史经历对于威胁感知的影响在于记忆。有被侵略历史的民众更可能形成对发动侵略国家的威胁感知。② 关于过去的历史冲突一旦被提起,也能引发对相关国家的威胁感知。③

从政治因素分析的学者们关注于政治制度、政党类别等方面的影响。如有研究认为,相似政治制度的国家之间安全威胁感知低,而不同政治制度的国家之间则威胁感知较高。④ 但也有学者通过实证检验得出了不同的结论,发现制度差异并没有显著影响大众对战争的支持态度,反而是冲突本身

---

① Valerie A. Sulfaro and Mark N. Crislip, "How Americans Perceive Foreign Policy Threats: A Magnitude Scaling Analysis," *Political Psychology*, Vol. 18, No. 1, 1997, pp. 103-124.

② 阎梁:《威胁认知、主权干预与中欧战略合作》,载《欧洲研究》,2008 年第 4 期,第 66 页。

③ A. Kupatadze and T. Zeitzoff, "In the Shadow of Conflict: How Emotions, Threat Perceptions and Victimization Influence Foreign Policy Attitudes," *British Journal of Political Science*, 2019, pp. 1-22.

④ Barbara Farnham, "The Theory of Democratic Peace and Threat Perception," *International Studies Quarterly*, Vol. 47, No. 3, 2003, pp. 395-415; Peter Gries et al., "A New Measure of the 'Democratic Peace': What Country Feeling Thermometer Data Can Teach us about the Drivers of American and Western European Foreign Policy," *Political Research Exchange*, Vol. 2, No. 1, 2020, pp. 1-11, https://doi.org/10.1080/2474736X.2020.1716630, 访问时间:2024 年 9 月 6 日。

具有明显影响。[①] 除此之外，也有研究发现大众的政治立场倾向与威胁感知大小具有关联。[②]

威胁感知形成所依赖的条件对于大众安全威胁感知具有一定解释力。但是这类解释也存在缺陷，无法说明同样的威胁依赖条件下，大众威胁感知为何仍然会变化和波动。例如，对于伊朗和以色列来说，两国相关的政治因素、文化和历史经历都是确定的常量，但以色列大众的威胁感知却并非一成不变。根据特拉维夫大学国家安全研究中心的调查，在 2018—2019 年的调查中有 20％的受访以色列民众认为伊朗核问题是以色列面临的最严重外部安全威胁，而在 2020—2021 年的调查中，这一比例上升到了 31％。[③] 可见，威胁依赖条件这一视角的解释无法较好地说明大众安全威胁感知波动和变化的原因。

（三）安全威胁感知的社会建构

除了外部客观来源、依赖的内部条件之外，一派学者转向社会建构角度解释安全威胁感知，这类研究可以分成三类，即身份认同、安全化视角以及媒体框架。

从身份认同视角分析的文献认为，在相同身份认同的情况下，威胁感知会下降，而身份认同不同的时候，威胁感知会更高。如有研究发现，共享的

---

① Femke E. Bakker, "Do Liberal Norms Matter? A Cross-regime Experimental Investigation of the Normative Explanation of the Democratic Peace Thesis in China and The Netherlands," *Acta Polit*, Vol. 2, No. 52, 2017, pp. 521-543.

② Nadim N. Rouhana and Susan T. Fiske, "Perception of Power, Threat, and Conflict Intensity in Asymmetric Intergroup Conflict: Arab and Jewish Citizens of Israel," *Journal of Conflict Resolution*, Vol. 39, No. 1, 1995, pp. 49-81.

③ Zipi Israeli and Ruth Pines, "National Security Index: Public Opinion, 2020—2021," The Institute for National Security Studies, Tel Aviv University, https://www.inss.org.il/wp-content/uploads/2021/01/Index-Public-Opinion.pdf, 访问时间：2024 年 10 月 13 日；Zipi Israeli, "National Security Index: Public Opinion Survey, 2018—2019," The Institute for National Security Studies, Tel Aviv University, https://www.inss.org.il/wp-content/uploads/2019/01/תילגנאב-ימואלה-וחטיבה-דדמ-2019.pdf, 访问时间：2024 年 10 月 13 日。

身份和价值观能够降低威胁感知。① 从安全化视角出发探究威胁感知的研究多关注大众如何接受建构的威胁,以及在这个过程中大众威胁感知如何变化。例如,有研究发现,过往经历中所得经验等因素能够影响大众威胁感知。② 大众从三个角度理解威胁,分别是联系性、确定性和矛盾性,他们的威胁感知也基于这些而发生变化。③在政府的作用之外,敌人形象的建构和集体记忆中的威胁描述也对大众感知产生重要影响。④ 媒体对大众感知的塑造作用则主要在于媒体框架效应,不同的媒体框架对大众认知具有不同的影响效果。⑤ 然而,媒体框架对大众感知的影响具有时效性。一些研究发现,在一段时间之后,媒体框架效应会消失。⑥ 该结果说明了媒体框架对大众感知影响的局限。

从社会建构视角有助于理解大众安全威胁感知的形成和变化,但其也存在着一定不足。身份认同的分析与文化和历史经历的缺陷相似,无法说明同一种身份认同的情况下,安全威胁感知为何波动。而安全化视角主要

---

① David L. Rousseau and Rocio Garcia-Retamero, "Identity, Power, and Threat Perception: A Cross-National Experimental Study," *Journal of Conflict Resolution*, Vol. 51, No. 5, 2007, pp. 744-771; Stephanie M. Müller, David L. Rousseau and Rocio Garcia-Retamero, "The Impact of Value Similarity and Power on the Perception of Threat," *Political Psychology*, Vol. 33, No. 2, 2012, pp. 179-193.

② Christoph O. Meyer, "International Terrorism as a Force of Homogenization? A Constructivist Approach to Understanding Cross-National Threat Perceptions and Responses," *Cambridge Review of International Affairs*, Vol. 22, No. 4, 2009, pp. 647-666.

③ Marie Gillespie and Ben O'Loughlin, "News Media, Threats and Insecurities: An Ethnographic Approach," *Cambridge Review of International Affairs*, Vol. 22, No. 4, 2009, p. 681.

④ Elizaveta Gaufman, *Security Threats and Public Perception: Digital Russia and the Ukraine Crisis*, Cham: Springer International Publishing, 2017.

⑤ 聂静虹、李磊磊、王博:《承前启后:新闻评论之架构效果探究》,载《新闻与传播研究》,2013 年第 3 期,第 64—75 页。

⑥ James N. Druckman and Kjersten R. Nelson, "Framing and Deliberation: How Citizens' Conversations Limit Elite Influence," *The American Journal of Political Science*, Vol. 47, No. 4, 2003, pp. 729-745; 陆屹洲、马得勇:《媒体框架效应及其持续性——以中美经贸摩擦为议题的实验研究》,载《新闻大学》,2020 年第 11 期,第 50—65 页;候为刚:《媒体框架效应中的民众国家安全观——以经贸安全为议题的实验研究》,载《当代亚太》,2022 年第 4 期,第 95—96 页。

关注于安全威胁感知的确立形成阶段，缺少对安全威胁感知已经确立之后发展变化的解释力。媒体框架效应可以直观说明大众安全威胁感知如何形成变化，但无法说明同一框架下为何大众安全威胁感知时大时小。因此，以上解释都存在一定缺陷。

（四）安全威胁感知的心理建构

一些学者关注安全威胁感知的心理学属性，从心理建构的视角分析安全威胁感知，其中值得关注的是情绪因素对安全威胁感知的作用。越来越多的研究成果表明，情绪因素能够影响大众安全威胁感知。情绪化的媒体报道更能引发大众的威胁感知，使他们愿意支持鹰派外交政策。① 恐惧、愤怒和焦虑等不同的情绪对威胁感知确有作用，但它们的具体影响却存在差异。恐惧能够增强威胁感知，愤怒则作用相反，能够使人们低估威胁。② 焦虑能够促使人们去收集相关信息，强化人们的安全威胁感知。③ 需要注意的是，也有研究发现，愤怒情绪下人们更可能对威胁判断失误，将非威胁视作威胁。④ 可见，愤怒情绪对于威胁感知的作用较为复杂，其影响存在争论。总结来说，情绪因素的分析对于理解大众安全威胁感知具有启发性。然而，情绪因素常常是短时间的，难以长时间持续，不适合解释大众安全威胁感知的长期变化现象，因此这类解释同样存在着不足。

综上，现有关于大众安全威胁感知影响因素的研究主要是对大众威胁感知的“点”分析，而并非长时间段分析。已有研究对于大众安全威胁感知长期变化现象及其原因缺少较好的解释。这些不足的主要原因在于缺乏对

---

① Shana Kushner Gadarian, “The Politics of Threat: How Terrorism News Shapes Foreign Policy Attitudes,” *The Journal of Politics*, Vol. 72, No. 2, 2010, pp. 469-483.

② Jennifer S. Lerner et al., “Effects of Fear and Anger on Perceived Risks of Terrorism: A National Field Experiment,” *Psychological Science*, Vol. 14, No. 2, 2003, pp. 144-150.

③ Cengiz Erisen, *Political Behavior and the Emotional Citizen*, London: Palgrave Macmillan, 2018, pp. 183-207.

④ Jolie Baumann and David DeSteno, “Emotion Guided Threat Detection: Expecting Guns Where There are None,” *Journal of Personality and Social Psychology*, Vol. 99, No. 4, 2010, pp. 595-610.

时间因素的自觉关注。时间对事物的影响可能通过时序、也可能通过缓慢过程积累等途径。[①] 正如“铁杵成针”“滴水穿石”,一些变量的变化虽然缓慢,但经过时间的累积最终会对大众安全威胁感知产生影响。然而当前关于大众安全威胁感知的分析中显然缺少对时间因素的自觉分析。与以往研究相比,本文将大众安全威胁感知的分析立足于长时段下,引入时间因素的分析,探究长时间段下时间的累积引起了何种因素的变化并导致大众安全威胁感知钝化现象,分析其发生的条件及具体机制,以此推进大众安全威胁感知影响因素的相关研究。

三、大众安全威胁感知钝化条件及机制

(一)威胁感知与大众安全威胁感知钝化

在分析大众安全威胁感知钝化的发生条件及机制之前,有必要明确“威胁感知”[②]及“安全威胁感知钝化”的含义。现有一部分文献偏重“威胁”的内涵对其进行定义[③],另一部分则偏重“感知”内涵定义。[④] 本文结合两类文献的思路,将威胁感知定义为人们基于客观威胁现实,对其进行主观理解和判

① 保罗·皮尔逊著,黎汉基、黄佩璇译:《时间中的政治——历史、制度与社会分析》,江苏人民出版社 2014 年版,第 25—110 页。

② 对于威胁感知,其对应的英文单词是“Threat Perception”。在一些相关中文研究中,也使用“威胁认知”的说法,如邱美荣:《威胁认知与朝核危机》,载《当代亚太》,2005 年第 6 期,第 3—11 页;杨恕、王术森:《议题性质、威胁认知、共同利益与“可合作安全”》,载《国际安全研究》,2018 年第 2 期,第 3—22 页;丁思齐:《美国应对核扩散的行为逻辑》,载《国际观察》,2019 年第 5 期,第 76—99 页。

③ J. David Singer, “Threat-Perception and the Armament-Tension Dilemma,” pp. 94-96; David L. Rousseau and Rocio Garcia-Retamero, “Identity, Power, and Threat Perception: A Cross-National Experimental Study,” *Journal of Conflict Resolution*, Vol. 51, No. 5, 2007, pp. 744-771; 庞琴:《中美权力变化与美国公众对“中国威胁”的认知》,载《世界经济与政治》,2020 年第 7 期,第 75 页;巴里·布赞著、闫健、李剑译:《人、国家与恐惧——后冷战时代的国际安全研究议程》,中央编译出版社 2009 年版,第 138—144 页;丁思齐:《美国应对核扩散的行为逻辑》,第 83—84 页。

④ Christoph O. Meyer, *The Quest for a European Strategic Culture: Changing Norms on Security and Defence in the European Union*, New York: Palgrave Macmillan, 2006, p. 31; 邱美荣:《威胁认知与朝核危机》,载《当代亚太》,2005 年第 6 期,第 6 页。

断后形成的认知。

安全威胁感知钝化是人们对于安全威胁变化在感知上的非敏感化和迟钝化，反映出关于安全威胁严重性和危害性在认知上的低判。大众安全威胁感知钝化表现为四种情形。第一种情形是，在安全威胁没有进展的情况下，大众安全威胁感知总体下降。第二种情形为，在安全威胁发展的情况下，大众安全威胁感知总体下降。第三种情形为，虽然安全威胁在发展，但大众安全威胁感知却减速增长。减速增长是相对的，其表现为在安全威胁增长程度相同的情况下，相比于威胁确立或刚出现重大新变化时，此时大众安全威胁感知的上升程度变小。第四种情形为，安全威胁减弱，大众安全威胁感知加速下降。加速下降也是相对的，具体表现为在安全威胁减弱程度相同的情况下，此时引起的安全威胁感知下降程度高于威胁刚刚确立或出现重大新变化之时。如果符合以上四种情形中的任意一个，就认为出现了大众安全威胁感知钝化现象。可见，大众安全威胁感知钝化现象表现为安全威胁感知大小或增长速度的衰减，既包括安全威胁感知大小的下降，也包括增长速度的变小。

（二）安全威胁事件类型与安全威胁感知钝化

安全威胁事件是安全威胁在现实中具体化体现，大众对安全威胁最为直接的体验就是安全威胁事件。不同的安全威胁事件对大众安全威胁感知的影响存在差异，但一直以来安全威胁事件类型所受到的关注不足。对于威胁事件的认识，危机管理领域中对于危机事件的研究成果具有启发性。该研究领域的关键概念包括紧急事件（emergency）、危机（crisis）、灾难（disaster）等。赫尔曼·莱昂纳德（Herman B. “Dutch” Leonard）和阿诺德·豪伊特（Arnold M. Howitt）两人对紧急事件做了细致分类，提出其包括“常规紧急事件”（routine emergencies）和“危机性紧急事件”（crisis emergencies）两类。常规紧急事件经常发生，人们对其发生和后果有一定预测能力，能够进行相应的准备和应对。危机性紧急事件下，紧急事件的发生出人意料，全新的情形使得人们缺少相应的举措来应对，甚至识别危机也需要时间，对于事

件的后果难以预期。[①] 莱昂纳德和豪伊特对于紧急事件的类型划分对于我们认识安全威胁事件具有借鉴意义。本文认为,安全威胁事件可以分为两种类型,分别是新生威胁事件和重复威胁事件。

新生威胁事件。这类事件指的是安全威胁刚确立或出现重大新变化时发生的威胁事件。其核心特点是,新生威胁事件发生时,人们所面对的威胁情境是全新的,人们对于这类威胁事件缺少应对经验,对于事件发生的后果缺少预测能力。

重复威胁事件。随着安全威胁事件不断重复发生,新生威胁事件会演变成重复威胁事件。一般来说,新生威胁事件演化成重复威胁事件需要较长的时间。在重复威胁事件发生时,人们所面临的威胁情境不是新的,而是旧的。此时人们对安全威胁事件已经具备较为丰富的应对经验,对于事件后果具有了一定预测能力。

对于新生威胁事件和重复威胁事件的判定主要依据四个标准,分别是后果预测难度、应对经验是否成熟、威胁是否出现重大新变化以及是否具有日常性。新生威胁事件下安全威胁事件发生后果的预测难度较高,人们的应对经验不成熟,威胁出现了重大新变化,且安全威胁事件的发生对于大众来说不具备日常性。而在重复威胁事件下,大众对于安全威胁事件的后果预测难度较低,人们已经具有了较为丰富的应对经验,安全威胁没有发生重大新变化,安全威胁事件具有日常性。

新生威胁事件和重复威胁事件对于大众安全威胁感知的影响不同,新生威胁事件下大众安全威胁感知不钝化,而重复威胁事件下则会出现大众安全威胁感知钝化现象。需要注意的是,发生重复威胁事件时可对应威胁变化的三种情况。第一种情况是安全威胁在威胁事件发生时缓慢进展,但

---

① Herman B. "Dutch" Leonard and Arnold M. Howitt, "Routine or Crisis: The Search for Excellence," *Crisis/Response Journal*, Vol. 4, Issue 3, 2008, pp. 33-34, https://www.hks.harvard.edu/sites/default/files/centers/research-initiatives/crisisleadership/files/Routine%20or%20Crisis.pdf, 访问时间: 2024 年 10 月 19 日; Herman B. "Dutch" Leonard and Arnold M. Howitt, "Against Desperate Peril: High Performance in Emergency Preparation and Response," pp. 5-15, https://www.hks.harvard.edu/sites/default/files/centers/research-initiatives/crisisleadership/files/desperate_peril.pdf, 访问时间:2024 年 10 月 20 日。

是这些进展并没有造成安全威胁性质的重大变化，属于从 0 到 100 的积累，而不是从 0 到 1 的突变。第二种情况是不进展，即安全威胁事件反复发生但安全威胁没有进展。第三种情况是倒退，即安全威胁事件虽然重复发生，但安全威胁总体上发生倒退。如果重复威胁事件发生，安全威胁没有进展，那么大众安全威胁感知可能会缓慢下降，此时对应的是钝化的第一种情形。如果重复威胁事件发生，安全威胁在进展，那么大众安全威胁感知可能会下降或减速上升。此时发生的钝化是前文所述的第二或第三种情形。如果重复威胁事件发生，安全威胁出现倒退，那么此时大众安全威胁感知可能表现为加速下降，对应的是大众安全威胁感知钝化的第四种情形。表 1 汇总比较了两类安全威胁事件类型特征。

表 1　两类安全威胁事件类型特征比较

特征 / 类型	后果预测难度	应对经验成熟/不成熟	威胁是否出现重大新变化	日常性/非日常性
新生威胁事件	高	不成熟	是	非日常性
重复威胁事件	低	成熟	否	日常性

来源：作者自制。

（三）大众安全威胁感知钝化发生机制

不同安全威胁事件类型下大众安全威胁感知表现之所以不同，是因为时间因素在此发挥了影响。大众安全威胁感知钝化出现的机制在于，随着安全威胁事件的不断发生，大众对于安全威胁的信息增加、知识增长以及熟悉度上升，这降低了安全威胁的不确定性，进而降低了大众的恐惧心理，最终导致大众安全威胁感知钝化现象的出现。

时间因素主要通过三条具体路径影响大众安全威胁感知的变化。首先，伴随着安全威胁事件的不断发生，大众关于安全威胁的信息增加，而信息增加降低了安全威胁的不确定性。不确定性是一种关于威胁不可知的状态[①]，信息的缺失和不完全能够增加不确定性。相反，当信息较为充足时，不

① Brian C. Rathbun, "Uncertain about Uncertainty: Understanding the Multiple Meanings of a Crucial Concept in International Relations Theory," *International Studies Quarterly*, Vol. 51, No. 3, 2007, pp. 541-545.

确定性也会降低。关于威胁的信息指的是关于威胁如何发生、发展及变化相关的事实或数据。在安全威胁出现之后,随着安全威胁事件不断发生,关于威胁发生发展的相关信息会增加,而这些信息的增加能够降低关于安全威胁的不确定性。

其次,随着安全威胁事件的不断发生,大众关于安全威胁的知识增长,也会降低安全威胁的不确定性。关于安全威胁的信息和知识在内涵上不同。前者是关于安全威胁的数据或事实,是零碎且未经处理的。但后者则是经过人们处理和解释分析后得出的关于安全威胁系统化的认识。关于安全威胁的知识也能够影响安全威胁不确定性的大小。随着安全威胁事件的反复发生,人们关于安全威胁的知识也会随之增长。在此情况下,人们对于威胁事件发生后所造成的危害水平、发生过程等具有了更强的预测能力和应对能力,因而安全威胁的不确定性降低。

最后,随着安全威胁事件的不断发生,大众关于安全威胁的熟悉性会上升,进而降低大众对于安全威胁的不确定性。关于安全威胁的熟悉性指的是对安全威胁了解多少,即对安全威胁的熟悉程度。熟悉性反映出人们在心理上对安全威胁的一种适应过程,熟悉性高代表着人们对于安全威胁事件的习惯和适应状态程度高。当安全威胁事件反复多次发生时,人们会越来越习惯并适应安全威胁的存在,对于安全威胁的熟悉性上升。而熟悉性上升能够减弱大众对于安全威胁的不可知状态,降低关于威胁的不确定性。

如前所述,新生威胁事件发生时,大众所面临的是全新的威胁情境,对于威胁如何发生发展,人们缺少相关的信息、知识,对于威胁熟悉性低,缺乏应对威胁的经验和预测能力,威胁的不确定性较高,大众对于威胁的恐惧心理也较高。此时伴随威胁事件的发生,大众的安全威胁感知不会出现钝化现象。随着时间的发展,安全威胁事件不断发生,关于安全威胁的信息增加、知识增长,人们对于威胁的熟悉性上升,不确定性降低。此时人们对威胁的认识和应对经验增长,对于威胁能够造成的后果有了预测的能力,对于安全威胁的恐惧心理下降,因而出现钝化现象。

当安全威胁发生重大新变化时,人们对于安全威胁事件再次缺少相关的信息、知识,熟悉性下降,关于安全威胁如何发展以及造成后果大小预测难度变大,应对经验缺乏。此时安全威胁的不确定性上升,面对新的威胁情

境，人们的恐惧心理会再度上升，因此上一阶段由重复威胁事件引发的大众安全威胁感知钝化现象此时会中止。因此，伴随着安全威胁事件类型在新生威胁事件和重复威胁事件中的转换，大众安全威胁感知钝化现象也会时而出现，时而中止。图 2 展示了大众安全威胁感知钝化发生机制。

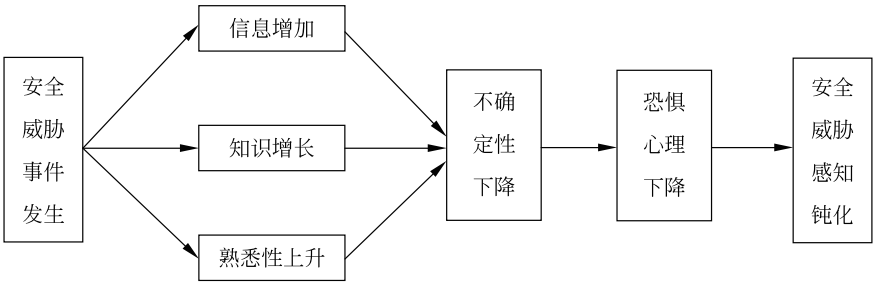

图 2 大众安全威胁感知钝化发生机制

来源：作者自制。

大众安全威胁感知钝化出现的原因符合心理学的已有研究结果。心理学的研究发现，人们对于新事物会投注更多的注意力，对于熟悉的事物注意力会下降。随着相似社会情境的反复发生，当这些情境再次发生时，人们更可能对其进行自动化反应。① 新的或出乎意料的刺激能吸引人们的注意力，突出和鲜明的刺激能影响人们对信息的加工，影响他们的知觉与记忆。② 近年新的研究发现，注意力和恐惧相关，越关注某一事物，就越能增加对某一事物的恐惧。人们对某一事物的更多关注能够导致对该事物具有更大的威胁感知。③ 当人们对威胁具有较少的信息和知识，熟悉性较低时，更可能对威胁事件投注更多的注意力，并出现更大的恐惧心理。相反，当人们对安全威胁的信息和知识较为丰富、对威胁较为熟悉时，他们对于威胁的关注可能

① 郑全全：《社会认知心理学》，浙江教育出版社 2008 年版，第 4 页。

② 罗伯特·L. 索尔索、M. 金伯利·马克兰、奥托·H. 麦克林著，邵志芳等译：《认知心理学（第 7 版）》，上海人民出版社 2008 年版，第 138 页；郑全全：《社会认知心理学》，第 127—132 页。

③ Kellen Mrkva, Jennifer C. Cole and Leaf Van Boven, "Attention Increases Environmental Risk Perception," *Journal of Experimental Psychology: General*, Vol. 150, No. 1, 2021, pp. 83-102.

更少,恐惧心理也更小。

大众安全感知在现实中受到多种因素影响,为了更好地认识和描述其长期变化规律,在此假定其仅受安全威胁和时间因素的影响,且安全威胁在长时间内经历了如下变化:在确立时期安全威胁增长,之后一段时间不进展。随着时间发展,安全威胁又出现了一次升级,且升级之后不再进展。那么,相对应的大众安全威胁感知将在安全威胁刚确立时与安全威胁的增长处于同步上升趋势。随着时间的发展,大众关于安全威胁的信息和知识不断积累,熟悉性上升,安全威胁事件类型演化为重复威胁事件。大众安全威胁感知将可能随着时间缓慢下降,出现钝化现象。随着威胁出现升级,安全威胁事件再度转变为新生威胁事件,大众安全威胁感知可能会随着威胁的发展而上升。当安全威胁不再进展,威胁事件类型演化为重复威胁事件时,大众安全威胁感知钝化现象将再度出现。这就是大众安全威胁感知变化的理想模型(图 3)。

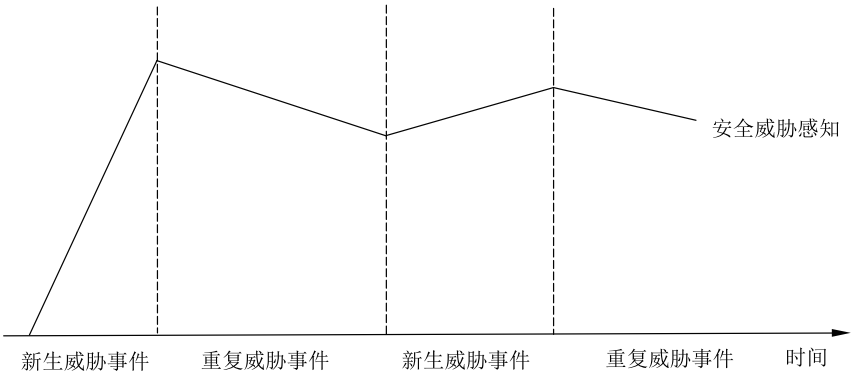

图 3 大众安全威胁感知随时间变化的理想模型

来源:作者自制。

(四)假设检验与操作化

根据以上理论观点,本文提出以下假设:

假设 1: 安全威胁确立后,当新生威胁事件发生时,大众安全威胁感知不钝化。

假设 2：随着时间发展，当重复威胁事件发生时，大众安全威胁感知钝化现象出现。

除此之外，本文也将在案例中考察大众安全威胁感知钝化发生的机制，即考察在安全威胁事件反复发生的情况下，信息增加、知识增长与熟悉性上升对于大众关于威胁不确定性的影响，以及是否造成恐惧心理的下降。

如前文所述，新生威胁事件和重复威胁事件在后果预测难度高低、应对经验是否成熟、威胁是否发生重大新变化、是否具有日常性这四个方面存在差异，因此在对两类事件类型进行判断时，也主要依据这四个维度判定。具体来说，在后果预测难度上，主要观察安全威胁事件造成或潜在的危害后果大小和过程是否难以预测。如果是，则预测难度高。对于应对经验是否成熟，则观察以下几个指标，分别是政府是否出台专门针对威胁的法律或政策，或建立专门应对机构组织；政府是否能够在威胁事件发生时较好应对，即是否存在较完善的应急响应方案。如果同时满足以上指标，则可以认为应对经验较为成熟。

对于威胁是否发生重大新变化，从是否出现“新变化”以及该变化是否“重大”来考察。对于“新变化”的判断，主要依据以下几个方面：威胁事件的发起者或者受害对象是否出现新变化；威胁的方式手段是否有新变化；引发危害的路径是否发生新变化；威胁危害程度是否显著变化，包括威胁事件引发的危害规模、危害程度或发生频次是否急剧变化。满足以上几方面之一则认为出现新变化。对于是否出现“重大”变化的判断，则依据以下两个指标：第一，该新变化是否改变了国家对于威胁的认知。如果改变了国家对于威胁的认知，则认为是重大变化。第二，该变化是否导致政府采取不同寻常的应对政策或影响国家安全议程设置。如果是，则认为是重大变化。威胁事件发生重大新变化需同时满足“新变化”和“重大”的标准。

对于安全威胁事件是否具有日常性，主要考察相似安全威胁事件的发生频次高低和数量多少。如果已经发生的相似安全威胁事件出现频率较高，事件发生数量较多，则认为这类事件具有日常性。相反，如果已发生的相似安全威胁事件数量较少，频率较低，则认为这类威胁事件为非日常性。

总之，在对安全威胁事件类型进行判断时，主要依据以上指标。如果后果预测难度高，应对经验不成熟，威胁发生重大新变化且不具有日常性，那

么则为新生威胁事件。反之,如果后果预测难度低、应对经验成熟、威胁没有发生重大新变化以及具有日常性,则认为是重复威胁事件。表 2 为安全威胁事件类型判断维度和指标总结。

表 2 安全威胁事件类型判断维度和指标总结

特征维度	判断指标
后果预测难度	威胁事件造成或潜在的危害后果是否难以预测
	威胁事件发生的过程是否难以预测
应对经验是否成熟	政府是否出台了针对威胁的法律或政策;或是否建立专门应对该威胁的组织机构
	政府已有的应对举措能否较好地处理威胁事件
威胁是否出现重大的新变化	威胁发起者和受害者、威胁手段以及引发危害的路径等与以往相比是否明显不同;或威胁造成或潜在的危害后果是否不同以往,具体表现为规模急剧扩大/缩小,或危害程度大幅加深/减轻,或威胁事件发生频次急速上升/下降等
	威胁新变化是否改变国家认知、影响国家安全议题设置和引发政府采取不同寻常的行动
是否具有日常性	相似威胁事件已发生频率高低
	相似威胁事件已发生数量多少

来源:作者自制。

对于安全威胁感知钝化现象的判定,首先需要符合三个条件。首先,在钝化现象发生时,安全威胁感知的变化总体趋势和安全威胁发展趋势不同步或不同速率。其次,安全威胁感知的变化必须表现为衰减,这可能是安全威胁感知大小的衰减或是增长速度的衰减。最后,钝化现象是一种长期趋势,必须持续一段时间,而不是仅在某一时间点上衰减。这种时间长度应当至少持续两年,否则难以判定安全威胁感知的衰减是否受到了短期因素的干扰,还是确实发生了钝化现象。

大众对于安全威胁的认识来源和领导人与专家精英不同。对于大众来说,他们对于安全威胁的认识主要通过安全威胁事件。大众对于安全威胁的认识实际上是安全威胁事件中所呈现出的威胁。因此本文对于安全威胁发展的判断也主要依据安全威胁事件本身及其引发的危害水平变化。也就

是说，安全威胁进展对应的是安全威胁事件中反映出的威胁危害水平上升，安全威胁不进展指的是安全威胁事件中反映出的威胁危害水平维持现状，而安全威胁倒退则对应的是安全威胁事件中反映出的威胁危害水平下降。对于那些大众容易直接经历后果的安全威胁的危害水平，本文主要关注以下指标进行衡量，分别是安全威胁事件发生次数以及后果严重程度。后果严重程度指的是威胁事件所造成人员伤亡或财产损失大小。本文将以年为单位对以上指标分别进行衡量和计算，并比较分析。对于那些大众难以直接亲身经历的安全威胁，如核武器威胁，对其威胁危害水平的衡量根据该威胁潜在的危害水平来分析，具体则依据安全威胁造成危害技术的发展情况以及威胁发起方的进攻意图大小，同样以年为分析单元。

以上便是大众安全威胁感知钝化判断时必须符合的三个条件以及安全威胁水平的衡量方法。在此基础上，如果大众安全威胁感知的变化符合文中所提出钝化的四种情形之一，则认为发生了安全威胁感知钝化现象。

在研究方法上，将以美国和意大利关于网络攻击威胁的大众威胁感知变化，以及法国大众对于恐怖主义威胁的感知变化为例进行假设检验，说明大众安全威胁感知钝化出现条件以及机制。对于网络攻击的案例，将具体分析 2015—2022 年美国和意大利大众对网络攻击威胁的感知变化。选择这两个国家的原因在于，两者都是西方发达国家，在政治制度、经济水平、社会文化等方面具有相似性，能够控制这些因素的影响。除此之外，为了检验假设 1 和假设 2，需要案例中存在没有发生钝化和发生钝化两种情况，而美国和意大利符合此种条件。且在所研究时间段内，美国和意大利关于网络攻击事件和大众威胁感知的数据较为连续和完整，能够提供深入分析的数据和材料。

对于恐怖主义威胁的案例，将具体分析“9·11”事件之后的法国恐怖主义威胁及大众安全威胁感知变化。选择法国作为案例分析对象的原因在于，法国首先符合恐怖主义威胁长期存在这一条件，如此才可能观察大众安全威胁感知的长期变化规律；且作为欧洲的大国，恐怖主义威胁在法国的发展历程具有代表性。除此之外，法国在恐怖主义威胁及大众安全威胁感知方面也具有连续十年以上且质量较高的数据。通过对法国案例的分析，有助于分析大众安全威胁感知长期变化的规律及机制，检验本文所提出的假设。

四、网络攻击威胁[①]与美意大众安全威胁感知变化

(一) 美国网络攻击威胁的发展及大众威胁感知变化

美国的网络信息化发展较早,早在 20 世纪 80 年代,美国就已经出现网络攻击事件。[②] 1988 年,美国发生莫里斯蠕虫病毒攻击事件,引起了约 6000 台电脑的损坏以及严重的财物损失。[③] 美国在此之后也开始意识到网络安全的重要性,并首次设立了计算机应急小组进行应对。[④] 进入 20 世纪 90 年代,美国的网络攻击威胁继续发展,出现了多起较为严重的网络攻击活动。如被美国政府称为“月光迷宫”(Moonlight Maze)的网络攻击事件。[⑤]

随着网络攻击威胁的发展,美国政府也逐步意识到自身在网络安全方面的脆弱性并采取行动。1998 年,克林顿签发 PDD-63 总统令,提出要在 2003 年获得保护国家基础设施免受网络攻击危害的能力,并针对基础设施

---

① 对于网络攻击的定义,当前存在着不同的认识,有广义和狭义之分。狭义的网络攻击强调对网络系统的破坏行为;广义的定义则将其看作一种手段,认为网络攻击包括网络犯罪、网络情报窃取、网络战等以网络攻击为发起手段的行为。本文采取广义的网络攻击定义。

② “First Incident of Cyber-espionage,” https://www.guinnessworldrecords.com/world-records/612868-first-incident-of-cyber-espionage, 访问时间:2024 年 10 月 26 日; Tom Fogden, “A Brief History of State-Sponsored Hacking,” March 12, 2019, https://tech.co/news/brief-history-state-sponsored-hacking-2018-11, 访问时间:2024 年 10 月 26 日。

③ Omry Haizler, “The United States' Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking,” *Cyber, Intelligence, and Security*, Vo.1, No.1, 2017, pp.31-43;程群:《美国网络安全战略分析》,载《太平洋学报》,2010 年第 7 期,第 73 页。

④ Christopher Whyte and Brian Mazanec, *Understanding Cyber Warfare: Politics, Policy and Strategy*, London: Routledge, 2019, p.210; Omry Haizler, “The United States' Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking,” *Cyber, Intelligence, and Security*, Vo.1, No.1, 2017, p.34.

⑤ Christopher Whyte and Brian Mazanec, *Understanding Cyber Warfare: Politics, Policy and Strategy*, pp.103-105.

保护的目标进行政府组织的调整。[①] 2003 年，美国首次出台了网络安全战略文件《确保网络空间安全国家战略》，提出网络安全的战略目标。[②] 2009 年，美国政府又出台了《网络空间政策评估：确保可靠和有弹性的信息与通信基础设施》文件。[③] 奥巴马政府时期，美国设立了国家网络安全协调官[④]，建立了网络司令部等。[⑤] 特朗普第一任期，美国网络司令部的地位又进一步得到提升。[⑥] 到了拜登政府时期，美国积极推进与盟友在网络安全方面的合作，追求美国在网络空间规则制定上的领导地位。[⑦]

从以上回顾可以看到，美国网络攻击威胁发展历史较长，已具有较丰富的经验来应对威胁。在美国，网络攻击事件已具有日常性，相似威胁事件发生的频率较高，发生的数量也较多。根据相关网络攻击数据库数据计算结

---

① *Critical Infrastructure Protection*, Presidential Decision Directive/NSC-63, May 22, 1998, https://irp.fas.org/offdocs/pdd/pdd-63.htm, 访问时间：2023 年 5 月 29 日。

② *The National Strategy to Secure Cyberspace*, The White House, February 14, 2003, https://www.hsdl.org/c/tl/national-strategy-secure-cyberspace/, 访问时间：2024 年 9 月 26 日。

③ *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, The White House, May 29, 2009, https://irp.fas.org/news/2009/05/cyber-fs.html, 访问时间：2023 年 5 月 31 日。

④ 张加军：《美任命“网络沙皇”凌驾于政府情报部门之上》，2009 年 12 月 25 日，来源：https://mil.huanqiu.com/article/9CaKrnJmOmB，访问时间：2024 年 10 月 27 日；《奥巴马任命“网络沙皇”》，2009 年 12 月 23 日，来源：https://news.ifeng.com/c/7fYgKkMA1Rs，访问时间：2024 年 10 月 27 日。

⑤ 李明海：《美军网络司令部的演变与启示》，2016 年 12 月 22 日，来源：http://www.cac.gov.cn/2016-12/22/c_1120164344.htm?from=timeline，访问时间：2024 年 10 月 1 日。

⑥ 《特朗普宣布美军网络司令部升级以提升国防水平》，2017 年 8 月 19 日，来源：https://m.huanqiu.com/article/9CaKrnK4Mbk，访问时间：2024 年 3 月 1 日；Jordan Fabian and Morgan Chalafant, “Trump Boosts US Cyber Command,” August 18, 2017, https://thehill.com/policy/cybersecurity/347085-trump-boosts-us-cyber-command/, 访问时间：2024 年 3 月 1 日。

⑦ 凌胜利：《拜登政府对华网络空间政策与中国应对》，载《和平与发展》，2022 年第 1 期，第 50 页。

果,从 2014 年到 2022 年,美国每年网络攻击事件总数始终居于各国首位。[①] 这些网络攻击事件虽然数量众多,但具有相似性。对于网络攻击威胁事件所能造成的危害后果及过程,预测难度较低。例如,2012 年,美国著名公司领英(LinkedIn)遭遇网络攻击,该攻击造成该公司用户密码泄露,涉及的密码数量高达 650 万。[②] 2019 年,美国第一资本金融公司(Capital One)遭遇黑客攻击,造成约 1 亿用户信息泄露。[③] 这些网络攻击事件极为相似。再如,2014 年,美国知名办公用品公司史泰博(Staples Inc)遭受恶意软件的攻击,超过 100 家门店共 116 万用户信息泄露。[④] 2021 年,美国互联网券商平台罗宾汉(Robinhood)受到网络入侵,700 万用户遭到信息泄露。[⑤] 这些网络攻击事件发生在不同的年份,但受害者数量众多,受害范围广泛,且事件之间具有较大的相似性。美国的网络攻击威胁事件类型已经演化为了重复

---

① CISSM Cyber Attacks Database, University of Maryland, https://cissm.umd.edu/cyber-events-database, 访问时间:2024 年 11 月 5 日;Nancy Gallagher and Charles Harry, "Classifying Cyber Events," pp. 17-31。

② Jaikumar Vijayan, "Hackers Crack More than 60% of Breached LinkedIn Passwords," June 7, 2012, https://www.computerworld.com/article/2504078/hackers-crack-more-than-60--of-breached-linkedin-passwords.html#:~:text=In%20all%2C%20a%20total%20of%206.5%20million%20hashed,identified%20about%205.8%20million%20hashed%20passwords%20as%20unique., 访问时间:2024 年 10 月 20 日。

③ Carnegie Endowment for International Peace, "Timeline of Cyber Incidents Involving Financial Institutions," https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline, 访问时间:2023 年 12 月 2 日;Rob McLean, "A Hacker Gained Access to 100 Million Capital One Credit Card Applications and Accounts," https://edition.cnn.com/2019/07/29/business/capital-one-data-breach/index.html, 访问时间:2024 年 10 月 20 日。

④ Associated Press, "Staples Customer Data Exposed in Security Breach," December 19, 2014, https://www.latimes.com/business/la-fi-staples-breach-20141219-story.html, 访问时间:2023 年 5 月 28 日;"Staples: 6-Month Breach, 1.16 Million Cards," https://krebsonsecurity.com/2014/12/staples-6-month-breach-1-16-million-cards/, 访问时间:2023 年 5 月 28 日。

⑤ "Robinhood Says Hackers Stole Data Belonging to 7 Million Customers," November 9, 2021, https://www.cbsnews.com/news/robinhood-data-breach-security-personal-data-hackers/, 访问时间:2023 年 6 月 30 日。

威胁事件，具备重复威胁事件的特征。

随着相似网络攻击事件的不断发生，人们对于这类网络攻击事件的信息增加，知识增长，熟悉性上升，恐惧心理下降。从已有的调查数据来看，美国民众已经出现了威胁感知钝化现象。对于网络攻击威胁的衡量，本文采取的数据来自美国马里兰大学的网络攻击数据库（CISSM Cyber Attacks Database）[①] 和美国战略与国际研究中心（Center for Strategic and International Studies，简称 CSIS）关于重大网络攻击事件的总结报告。[②] 对于网络攻击威胁水平的衡量，本文将以上两个数据库的数据以年为单位分别进行了统计，计算出了美国每年遭遇的网络攻击次数和重大网络攻击次数。[③] 由于重大网络攻击事件相比于一般网络攻击事件更能反映出网络攻击威胁的严重程度，对大众威胁感知的影响更大，因此在计算权重时，设置网络攻击次数和重大网络攻击次数的权重为 1∶10，并对此进行加总计算最终得到网络攻击威胁指数[④]，以此衡量和比较威胁事件危害程度，说明网络攻击威胁进展情况。

本文关于美国民众对网络攻击的威胁感知数据来自皮尤研究中心的全

---

① CISSM 网络攻击数据库的数据从 2014 年开始，该数据库同时采用机器编码和手动编码的方式，具体来说，使用机器自动抓取网络新闻等来源中的网络攻击事件，同时结合研究人员手动编码。详见："CISSM Cyber Events Database," Center for International & Security Studies at Maryland, https://cissm.umd.edu/cissm-cyber-events-database, 访问时间：2024 年 9 月 24 日。

② CSIS 将针对政府、军队和高科技企业，或者造成损失达到 100 万美元以上的网络攻击事件定义为重大网络攻击事件。详见 Center for Strategic and International Studies（CSIS），"Significant Cyber Incidents Since 2006," https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents，访问时间：2024 年 10 月 28 日。

③ 由于网络攻击事件具有难以溯源的特征，本文仅参考 CSIS 报告中关于网络攻击事件发生次数和年份的信息，其他信息未采用。因为一些网络攻击事件的发生时间不容易确定，所以本文以 CSIS 报告中宣告网络攻击事件的时间作为网络攻击事件发生的年份。

④ 对于这两个指标的权重，本文也使用了 1∶3，1∶5，1∶8，1∶15，1∶20，1∶30 等来计算威胁指数。最终发现比例的设置不影响对钝化现象的判断结果。可见，对网络攻击威胁指数的计算结果较为稳健，其权重设置并不影响是否出现钝化现象的判断。

球主要安全威胁大众问卷调查。[①] 2015 年,有 59%的美国民众相信网络攻击威胁是国家安全的主要威胁。2016 年,选择网络攻击的美国民众比例增长到了 72%,到了 2018 年小幅度增长至 74%。在 2020 年的调查中,该比例仍为 74%。2022 年,认为网络攻击是美国最主要的安全威胁的民众比例下降为 71%。从美国网络攻击威胁发展趋势及大众威胁感知的变化来看,虽然网络攻击威胁在快速发展,但美国民众的安全威胁感知并非同步发展,甚至有所下降。可见,美国大众关于网络攻击威胁的感知出现了钝化现象。

通过对美国网络攻击威胁发展及威胁事件类型的分析,可以看出美国的网络攻击威胁发展历史长、网络攻击威胁事件数量多、发生频次高。网络攻击事件已经演化为了重复威胁事件。美国的网络攻击威胁事件后果预测难度低,应对经验较为成熟,网络攻击威胁没有发生重大新变化,威胁事件的发生具有日常性。随着大量相似性网络攻击威胁事件的发生,美国大众也确实出现了安全威胁感知的钝化现象。图 4 列示了 2015—2022 年美国大众威胁感知变化与网络攻击威胁指数变化。

---

① Jill Carle, "Climate Change Seen as Top Global Threat 2015," Pew Research Center, July 14, 2015, https://www.pewresearch.org/global/2015/07/14/climate-change-seen-as-top-global-threat/, 访问时间:2022 年 9 月 15 日;Jacob Poushter and Dorothy Manevich, "Globally, People Point to ISIS and Climate Change as Leading Security Threats," Pew Research Center, August 1, 2017, https://www.pewresearch.org/global/2017/08/01/globally-people-point-to-isis-and-climate-change-as-leading-security-threats/, 访问时间:2022 年 9 月 17 日;Jacob Poushter and Christine Huang, "Climate Change Still Seen as the Top Global Threat, But Cyberattacks a Rising Concern," Pew Research Center, February 10, 2019, https://www.pewresearch.org/global/2019/02/10/climate-change-still-seen-as-the-top-global-threat-but-cyberattacks-a-rising-concern/, 访问时间:2022 年 9 月 25 日;Jacob Poushter and Christine Huang, "Despite Pandemic, Many Europeans Still See Climate Change as Greatest Threat to Their Countries 2020," Pew Research Center, September 2020, https://www.pewresearch.org/global/2020/09/09/despite-pandemic-many-europeans-still-see-climate-change-as-greatest-threat-to-their-countries/, 访问时间:2022 年 10 月 28 日;Jacob Poushter, Moria Fagan and Sneha Gubbala, "Climate Change Remains Top Global Threat Across 19-Country Survey," Pew Research Center, August 31, 2022, https://www.pewresearch.org/global/2022/08/31/climate-change-remains-top-global-threat-across-19-country-survey/, 访问时间:2023 年 4 月 28 日。

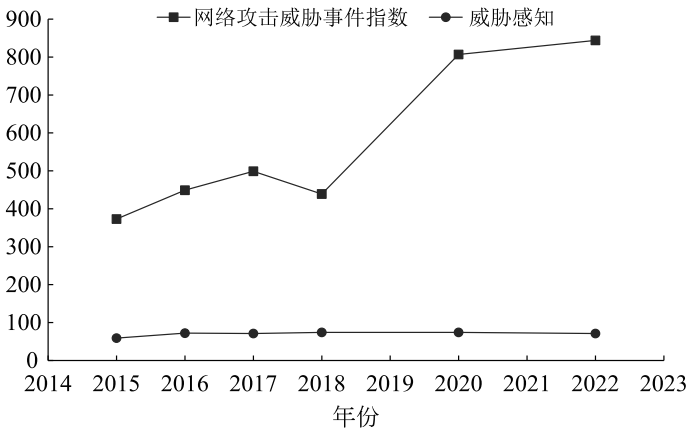

图 4 美国大众威胁感知变化与网络攻击威胁指数变化

注：由于该大众威胁感知调查的时间每年不固定，而大众对于网络攻击威胁的感知以从前发生的威胁事件为基础，因此本文在对威胁感知和网络攻击威胁指数进行比较时，将威胁感知数据和前一年的网络攻击威胁指数进行对应分析。如在图中，2015 年的大众威胁感知数据对应的是 2014 年的网络攻击威胁指数。

来源：作者自制。

（二）意大利网络攻击威胁的发展及大众威胁感知变化

相比于美国，意大利的网络攻击威胁发展得较晚，但近几年快速发展，形势日益严峻。意大利信息安全协会(Clusit)在 2016 年曾评估，认为意大利已出现了网络犯罪历史最严重水平。然而在 2022 年上半年，意大利网络犯罪水平被刷新，再创历史纪录。[①] 不止如此，意大利的网络攻击事件总体数量也在迅

① “First Half of 2022 Worst ever for Cybercrime,” ANSA Italy, November 9, 2022, https://www.ansa.it/english/news/general_news/2022/11/09/first-half-of-2022-worst-ever-for-cybercrime-report_6d89d114-c280-49e5-94ee-aafc4ab7fe52.html, 访问时间：2024 年 11 月 14 日；“Worst-ever Semester for Cyberattacks,” ANSA Italy, October 4, 2018, https://www.ansa.it/english/news/science_tecnology/2018/10/04/worst-ever-semester-for-cyberattacks_a7d5fac3-d05c-41b2-982f-85e1f3f6cea4.html, 访问时间：2024 年 11 月 14 日；“2016 Worst Year ever for Cybercrime Report,” ANSA Italy, February 22, 2017, https://www.ansa.it/english/news/2017/02/22/2016-worst-year-ever-for-cybercrime-report_ea534f81-3563-463f-8977-ce18eeb9a5dd.html，访问时间：2024 年 11 月 14 日。

速增长。2018 年,意大利平均每月发生 106 件网络攻击事件。到了 2020 年 12 月,该数字已达到 227 件,[①]网络攻击的增长速度也迅速上升。据相关报道,相比于 2021 年,2022 年意大利的网络攻击事件总量增长了 138%。[②]

意大利的网络攻击事件不仅数量增多,后果也日益严重。例如,2017 年 7 月,意大利最大的银行裕信银行(UniCredit)遭遇黑客袭击,导致 40 万客户信息被泄露。[③]再如,2018 年意大利知名海底工程和建筑公司塞班(Saipem)在中东、印度、意大利等地服务器被黑客用一种叫作沙蒙(Shamoon)的病毒攻击,导致公司数百台电脑瘫痪。[④] 2021 年 8 月,意大利出现了公共卫生领域中最大的一起网络攻击事件:拉齐奥大区卫生部门的计算机系统遇到网络攻击,同时政府还遭到了不明来源的黑客的勒索。[⑤]

面对网络攻击威胁的发展,意大利也在进行应对。2013 年,意大利出台了

---

① Oren Elimelech, "Cyber Threats & Ransomware Attacks in Italy Europe," CyberTeam360, https://www.ordineavvocatiroma.it/wp-content/uploads/2021/01/Italy.pdf,访问时间:2023 年 9 月 14 日。

② "Italy Says Cyber Attacks on the Rise Since Invasion of Ukraine," September 9, 2022, https://tech.hindustantimes.com/tech/news/italy-says-cyber-attacks-on-the-rise-since-invasion-of-ukraine-71662113906933.html, 访问时间:2023 年 9 月 14 日;"Cyber-attacks in Italy up 138% after Ukraine War," ANSA, January 3, 2023, https://www.ansa.it/english/news/general_news/2023/01/03/cyber-attacks-in-italy-up-138-after-ukraine-war_1c9eec3c-63b6-4e7b-8ba4-e6ab79fd47d4.html, 访问时间:2023 年 9 月 14 日。

③ Pappi Hex, "Italy's Largest Bank, UniCredit Suffers Data Breach, 400,000 User Accounts Affected," July 27, 2017, https://www.cybersecurity-review.com/news-july-2017/unicredit-bank-hacked-400000-accounts-exposed/,访问时间:2023 年 6 月 14 日。

④ Stephen Jewkes and Jim Finkle, "Italian Oil Services Firm Saipem Blames Cyber Attack on Shamoon Virus Variant," December 13, 2018, https://www.insurancejournal.com/news/international/2018/12/13/511880.htm, 访问时间:2023 年 6 月 14 日。

⑤ "Italian Website for Vaccination Appointments Targeted by Hackers," August 2, 2021, https://www.euronews.com/2021/08/02/italian-website-for-vaccination-appointments-targeted-by-hackers; Livia Borghese and Sharon Braithwaite, "Hackers Block Italian Covid-19 Vaccination Booking System in 'Most Serious Cyberattack' Ever," August 2, 2021, https://edition.cnn.com/2021/08/02/business/italy-hackers-covid-vaccine-intl/index.html#:~:text=Hackers%20have%20attacked%20and%20blocked%20an%20Italian%20Covid-19,cyberattack%20the%20country's%20health%20service%20has%20ever%20seen.,访问时间:2023 年 6 月 14 日。

《国家网络空间安全战略框架》文件(National Strategic Framework for Cyberspace Security),明确了维护网络安全的相关行动指南。[①] 2017 年,意大利更新了其网络安全行动计划,计划建立国家网络安全研发中心(National Cybersecurity R&D Center)、国家密码中心(National Cryptographic Center)等机构。[②] 2021 年,设立国家网络安全局(The National Cybersecurity Agency,简称 ACN),负责执行网络安全战略目标。[③] 2022 年,意大利又再次更新其网络安全战略,明确了网络安全治理框架。[④]

虽然意大利提出了应对网络攻击威胁的政策,但是实施并不充分。其在近年进行了一定改革[⑤],但并没有改变在网络安全方面的脆弱性。意大利仍缺乏应对重大网络攻击威胁的实践经验,网络安全治理机构分散,信息共享能力受限,公共部门网络基础设施陈旧,计算机软件和硬件落后,网络系统抗风险能力低,缺少网络安全专业知识培训和专业人员。[⑥] 可见,意大利

---

① *National Strategic Framework for Cyberspace Security*, December 2013, p. 10, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf, 访问时间:2023 年 9 月 5 日。

② *The Italian Cybersecurity Action Plan*, March 2017, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2019/05/Italian-cybersecurity-action-plan-2017.pdf

③ "About ACN," https://www.acn.gov.it/en/agenzia/chi-siamo, 访问时间:2023 年 6 月 28 日。

④ "National Cyber Security Strategy 2022—2026," https://www.acn.gov.it/ACN_EN_Strategia.pdf, 访问时间:2023 年 6 月 30 日。

⑤ "About ACN," https://www.acn.gov.it/en/agenzia/chi-siamo, 访问时间:2023 年 6 月 14 日;*National Cybersecurity Strategy 2022—2026*, https://www.acn.gov.it/ACN_EN_Strategia.pdf, 访问时间:2023 年 6 月 14 日。

⑥ Tommaso De Zan, Giampiero Giacomello and Luigi Martino, "Italy's Cyber Security Architecture and Critical Infrastructure," in Scott N. Romaniuk and Mary Manjikian, eds., *Routledge Companion to Global Cyber-Security Strategy*, London: Routledge, 2021, pp. 121-126; Giampiero Giacomello, "Va Pensiero: The Evolution of Italy's Information Society," in M. Evangelista ed., *Italy From Crisis To Crisis: Political Economy, Security and Society in the 21st Century*, London and New York: Routledge, 2018, p. 212; Federico Guerrini, "Fed up with Constant Cyberattacks, One Country is About to Make Some Big Changes," September 3, 2021, https://www.zdnet.com/article/fed-up-with-constant-cyberattacks-one-country-is-about-to-make-some-big-changes/; *Annual Report* 2022, ACN, https://www.acn.gov.it/documents/ACN_Relazione_2022_ENG.pdf, 访问时间:2023 年 12 月 24 日。

的应对经验并不完善,防御重大网络攻击的能力仍有不足。

近年来意大利遭遇的网络攻击的受害部门越来越多,包括教育部门、金融部门以及基础设施等,且网络攻击所运用的技术越来越复杂。① 意大利发生的网络攻击事件并非同类相似威胁事件的重复发生。在网络攻击对象日益多元化,攻击手段多样化且危害水平持续增长的情况下,网络攻击威胁事件的预测难度较高,且不具有日常性。如前所述,意大利网络攻击威胁的新变化已经引发了政府和社会的关注,也改变了政府对于网络安全的认知和行动,影响了政府安全议题。可见,当前意大利的网络攻击威胁具备新生威胁事件后果预测难度高、应对经验不成熟、出现重大新变化和非日常性的特征,威胁事件类型是新生威胁事件。

另一方面,意大利大众对于网络攻击威胁缺少相关信息和知识,熟悉度也较低。如前所述,意大利的网络系统管理人员尚缺少关于网络安全相关的专业知识培训,普通大众对于网络安全的知识和信息更少。在网络攻击威胁持续发生新变化的情况下,大众对于发生的网络攻击威胁熟悉性低,不确定性高。在意大利社会存在着对网络安全脆弱性的担忧。一些意大利学者便指出,当前的网络安全形势十分严峻,然而国家严重缺乏应对行动。②

---

① Rosanna Pittiglio et al., "Cybersecurity, Personal Data Protection and Crime Prevention from an Italian Perspective," in Seung Ho Park, Maria Alejandra Gonzalez-Perez and Dinorá Eliete Floriani, eds., *The Palgrave Handbook of Corporate Sustainability in the Digital Era*, Cham: Palgrave Macmillan, 2021, p. 135; Marco R. A. Bozzetti, Luca Olivieri and Fausto Spoto, "Cybersecurity Impacts of the Covid-19 Pandemic in Italy," paper delivered to TASEC'21: Italian Conference on CyberSecurity, April 7-9, 2021, http://sunsite.informatik.rwth-aachen.de/Publications/CEUR-WS/Vol-2940/paper13.pdf, 访问时间:2023 年 12 月 24 日。

② Federico Guerrini, "Fed up with Constant Cyberattacks, One Country is About to Make Some Big Changes," September 3, 2021, https://www.zdnet.com/article/fed-up-with-constant-cyberattacks-one-country-is-about-to-make-some-big-changes/, 访问时间:2023 年 12 月 20 日;Marco R. A. Bozzetti, Luca Olivieri and Fausto Spoto, "Cybersecurity Impacts of the Covid-19 Pandemic in Italy," paper delivered to TASEC'21: Italian Conference on CyberSecurity, April 7-9, 2021, http://sunsite.informatik.rwth-aachen.de/Publications/CEUR-WS/Vol-2940/paper13.pdf, 访问时间:2023 年 12 月 24 日; Martina Neri, Federico Niccolini and Rosario Pugliese, "Assessing SMEs' Cybersecurity Organizational Readiness: Findings from an Italian Survey," *Online Journal of Applied Knowledge Management*, Vol. 10, No. 2, 2022, pp. 1-22; Domitilla Vanni, "Are We any Good at Protecting Our Societies and Economies from the Threat of Economic Crime and Misconduct? A Look at the Italian System", *Journal of Financial Crime*, Vol. 26, No. 4, 2019, pp. 1006-1013.

意大利社会对于网络攻击威胁充满忧虑，且威胁感知处于上升趋势，这一点通过皮尤研究中心的大众问卷调查数据可以反映出来。使用与美国案例同样的数据来源与计算方式，本文也得到了意大利民众威胁感知变化与网络攻击威胁事件指数。由图 5 可见，在 2015 年的调查中，25％的意大利民众认为网络攻击是国家主要威胁，2016 年这一比例为 51％。2020 年的调查中，53％的意大利民众将网络攻击视为国家的主要安全威胁。在 2022 年新的调查中，该比例上升为 67％。

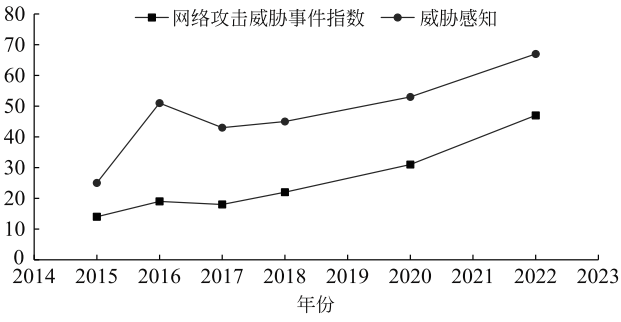

图 5 意大利大众威胁感知变化与网络攻击威胁指数变化

注：意大利的案例同美国一致，将威胁感知数据和前一年的网络攻击威胁指数进行对应分析。如在图中，2015 年的大众威胁感知数据同样对应的是 2014 年的网络攻击威胁指数。

来源：作者自制。

在本文研究的时间段内，意大利的网络攻击威胁处于上升趋势，而意大利民众的威胁感知也总体处于上升趋势，两者发展趋势相对一致。意大利民众对于网络攻击威胁的安全感知并没有出现钝化。

通过美国和意大利两个案例的比较，可以看到美国和意大利民众对网络攻击威胁感知的差别在于威胁事件类型不同。网络攻击威胁在美国已经演化成了重复威胁事件，而网络攻击威胁在意大利属于新生威胁事件。由于美国和意大利所属网络攻击威胁事件类型的差异，美国大众对于网络攻击的威胁感知已经出现了钝化现象，而意大利则没有出现钝化现象。通过美国和意大利的案例可以检验本文的假设 1 和假设 2。

五、恐怖主义威胁与法国大众安全威胁感知

(一) 美国“9·11”事件之后法国恐怖主义威胁的发展及大众威胁感知

美国“9·11”事件可以看作是法国恐怖主义威胁新阶段的一个开始,其改变了法国对于恐怖主义威胁的认识,法国政府自此将其提升到了国家安全的高度。① 法国政府认为反对恐怖主义是一场“战争”②,而并非像从前一样认为是国内犯罪。恐怖主义威胁的新变化下,法国大众缺少相关的知识、信息以及应对经验,此时威胁不确定性高,人们难以预料恐怖主义威胁事件何时以及如何发生,大众对于恐怖主义袭击的恐惧程度较高。为了安全考虑,法国街头的垃圾桶从金属垃圾桶变成了金属圈配透明塑料袋。③ 到了 2002 年的圣诞节期间,法国街头也少有行人,因为民众担心发生恐袭。④

为了应对恐怖主义威胁,法国政府采取了积极行动。2002 年,时任法国总统的希拉克重组了国内安全委员会,以提高政府应对重大危机事件的能力。萨科齐上台后成立了国防与国家安全委员会,该委员会作为国家安全的最高决策机关而存在。⑤ 2008 年,法国将领土监视局与情报总局合并,以提升工作效率并简化相关部门间的关系。⑥ 2009 年,法国还专门创建了用于应对恐怖袭击的精锐警察部队——“国家警察反应部队”。⑦ 法国也先后

---

① 凌胜利、胡碧钰:《21 世纪以来的法国反恐政策研究:观念、体系、举措与效果》,载《公安学研究》,2020 年第 4 期,第 54—55 页。

② Silvia D'Amato, *Cultures of Counterterrorism: French and Italian Responses to Terrorism after 9/11*, London: Routledge, 2019, Chaper 4, https://doi.org/10.4324/9780429465369, 访问时间:2023 年 9 月 1 日。

③ 张祝基:《法国 安全防范是关键》,载《人民日报》,2002 年 9 月 11 日,第 7 版。

④ 张祝基、陈立群:《忐忑不安迎新年》,载《人民日报》,2002 年 12 月 30 日,第 7 版。

⑤ 沈孝泉:《法国“反恐”催生国家安全机制》,来源:http://www.tzzzs.com/type_fmgs_post/3814.html,访问时间:2023 年 7 月 6 日。

⑥ 周秋君:《英法国内反恐情报机构改革的比较研究》,载《情报杂志》,2020 年第 11 期,第 12 页。

⑦ 熊世英、邱健:《法国反恐机制与力量概览》,载《现代军事》,2015 年第 4 期,第 49 页。

通过了一系列法律以积极反恐，如《日常安全法》(Every-Day Security Law)、《安全和边境管制反恐法》(Law for the Fight against Terrorism with Disposition on Security and Border Controls)和《安全和打击恐怖主义法》(Law on Security and Fight against Terrorism)。①

随着时间的发展，法国民众对于恐怖主义威胁感知开始出现钝化。从2010年开始到2013年，法国的恐怖主义威胁危害水平整体上升，但是这些威胁事件并非全新的威胁事件，而是相似的威胁事件。这一时期最主要发生的恐怖袭击事件是科西嘉岛上的恐怖袭击事件。例如2012年5月，科西嘉岛上发生了21起爆炸案，其规模在历史上较为罕见，造成了较大损害。②科西嘉岛上的这些恐怖袭击事件发生频繁，造成的客观损害在上升，但由于之前已经存在较多相似袭击事件，人们已经积累了丰富的应对经验，对这类袭击事件较为熟悉，因此即使恐袭事件造成的危害后果上升，法国大众对于恐怖主义的整体认识也并没有发生较大改变。

在2010—2013年间发生的恐怖袭击事件还包括2012年3月在图卢兹和蒙托班发生的恐怖袭击事件。该事件中，伊斯兰极端分子穆罕默德·梅拉赫(Mohammed Merah)袭击了士兵和学生并造成七人死亡。③ 该恐怖袭击事件在法国社会引起了较大关注，但并没有从根本上改变法国政府和民众对于恐怖主义威胁的认识。此时法国政府对于自身的反恐经验十分自信，其反恐政策和经验被认为是法国本土一直没有经历大规模恐怖袭击的重要原因。④ 其发生没有动摇法国政府的反恐信心，而法国大众也没有明显

---

① Silvia D'Amato, *Cultures of Counterterrorism: French and Italian Responses to Terrorism after 9/11*, London: Routledge, 2019, Chaper 3, https://doi.org/10.4324/9780429465369, 访问时间：2023年9月1日；凌胜利、胡碧钰：《21世纪以来的法国反恐政策研究：观念、体系、举措与效果》，第66页。

② "Twenty One Blasts over Weekend Rock Corsica," May 14, 2012, https://www.rfi.fr/en/france/20120514-twenty-one-blast-rock-corsica-over-weekend, 访问时间：2023年4月5日。

③ Adrien Morin, "The Mohammed Merah Case: Lessons Learned for French Domestic Intelligence?" November 18, 2017, https://theforeignanalyst.com/the-mohammed-merah-case-lessons-learned-for-french-domestic-intelligence/, 访问时间：2023年9月1日。

④ Pernille Rieker, *French Foreign Policy in a Changing World*, Cham: Palgrave Macmillan, 2017, p.144.

表现出对恐怖主义威胁的担忧。在该事件之后,萨科齐政府曾希望利用这起事件来强调恐怖主义形势的严峻性,并获得更多国内支持,然而却并没有成功。相关民调显示,在该事件发生前后,法国民众的关心事项中安全问题的排名始终靠后。①

法国民众这一时期对于恐怖主义威胁的钝化现象也清晰反映于相关数据中。对于法国恐怖主义客观威胁水平的衡量,全球恐怖主义指数(Global Terrorism Index,简称 GTI)提供了有益的启发。GTI 是澳大利亚著名智库经济与和平研究所(The Institute for Economics and Peace)根据 GTD 数据库②的数据计算出的关于全球各国受到恐怖主义影响的指数。③ 由于 GTI 所得结果考虑到了历史事件的心理影响,而本文只希望测量恐怖主义威胁水平的变化,因此其结果不能完全适用于本研究。本文部分借鉴了其计算方式,同样使用了 GTD 关于恐怖主义威胁事件的相关数据,包括事件发生次数、死亡人数、受伤人数和财产损失四个指标,并利用 GTI 的指标权重计算该四个指标④,得到 2001 年到 2019 年法国的恐怖主义威胁指数(图 6),以此反映客观威胁的变化结果。

关于法国民众对于恐怖主义威胁感知变化的数据,本文则使用了标准欧洲晴雨表(The Standard Eurobarometer)。欧洲晴雨表最初由欧盟委员

---

① Tracy McNicoll, "Why Toulouse Terror Fears Won't Help Sarkozy With Voters," March 30, 2012, https://www.thedailybeast.com/why-toulouse-terror-fears-wont-help-sarkozy-with-voters, 访问时间:2024 年 5 月 19 日。

② 全球恐怖主义数据库(Global Terrorism Database),简称 GTD。该数据库是关于恐怖主义研究中较为权威的公开数据库,见 Global Terrorism Database, University of Maryland, 2021, https://start.umd.edu/gtd/。

③ The Institute for Economics and Peace, 2012 *Global Terrorism Index*, p. 8.

④ 首先,在 GTD 数据中,根据是否是恐怖主义行为这一变量,在取值为不需要怀疑的数据中提取法国从 2001 年到 2019 年的相关数据,然后以国家-年为观察单元来计算法国每年恐怖主义事件发生次数、死亡人数、受伤人数和财产损失。以上四个指标权重分别为 1,3,0.5 和 2。接下来以每年恐怖主义事件发生次数、死亡人数、受伤人数和财产损失的数据分别和相应的权重相乘,之后相加,最后计算出恐怖主义威胁指数。在计算过程中,对于案例中的缺失数据,以及在"财产损失"标注为"未知"的数据,都赋值为 0。关于不同程度财产损失的赋值权重,本文参照了 GTI 的指标权重,详情可见 The Institute for Economics and Peace, *2012 Global Terrorism Index*, p. 9.

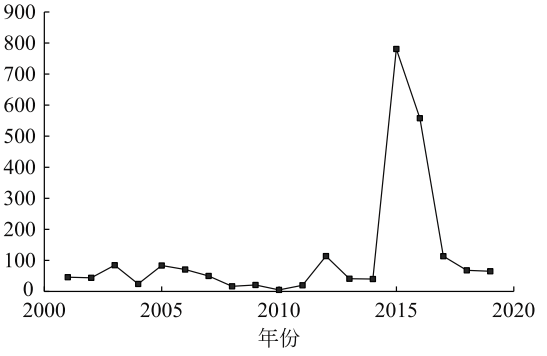

图 6 2001—2019 年法国恐怖主义威胁指数变化

来源:作者自制。

会于 1974 年发起。[①] 标准欧洲晴雨表每年调查两次,由于其调查的长期性、连续性,这项数据能够较好地反映法国民众的威胁感知变化。在调查中,其中有一个问题是“您认为我们的国家当前面临的两个最重要的问题是什么”,其中包括恐怖主义、气候变化等选项。本文将调查中选择恐怖主义的民众比例作为恐怖主义威胁感知的反映。[②]

图 7 展示了 2003—2019 年法国大众威胁感知变化。从法国恐怖主义威胁指数和大众安全威胁感知变化的整体走势来看,从 2003 年开始至 2009 年,法国恐怖主义威胁水平总体下降,大众安全威胁感知也处于下降趋势。而从 2010 年到 2013 年,法国恐怖主义威胁水平呈现上升趋势,但大众安全威胁感知处于下降趋势,法国大众对于恐怖主义威胁感知出现了钝化现象。[③]

可见,随着时间发展和恐怖主义威胁事件的不断发生,2010 年到 2013 年这一时间段,法国已经积累了较为丰富的反恐经验,恐怖主义威胁事件的

---

① “About Eurobarometer,” https://europa.eu/eurobarometer/about/Eurobarometer,访问时间:2024 年 10 月 26 日。

② 该问题从 2003 年的调查才开始出现,因此相关数据从 2003 年开始统计。欧洲晴雨表每年进行两次调查,因此本文以两次调查结果的平均值作为该年的数据。

③ 由于欧洲晴雨表的调查每年上半年和下半年各一次,基本能够反映出大众对当年的安全威胁变化的感知,因此在分析时并没有像前文网络攻击威胁案例那样,以威胁感知对应前一年安全威胁水平的方式。但即使以前一年的恐怖主义威胁指数对应当年的威胁感知数据进行分析,即使用 2009—2012 年的恐怖主义威胁指数数据对应 2010—2013 年恐怖主义威胁感知变化来分析,也同样可以看出发生了钝化现象,结果没有改变。

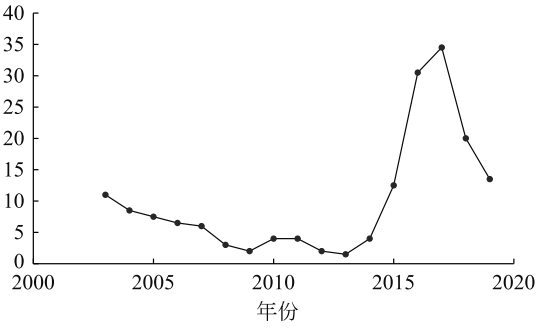

图 7 2003—2019 年法国大众威胁感知变化

来源:作者自制。

发生后果预测难度变低,恐怖主义威胁并没有发生重大新变化,在相似的恐怖主义威胁事件重复发生下,威胁事件具有日常性。恐怖主义威胁事件类型演化为重复威胁事件。这种情形下,法国民众对于恐怖主义威胁的知识增加,信息增多,熟悉度上升,恐惧心理下降,出现钝化现象。

(二)法国恐怖主义威胁的新变化及大众威胁感知

2015 年,法国国内恐怖主义形势再次发生了新变化。2015 年 1 月 7 日,恐怖分子袭击法国《查理周刊》杂志社并造成 12 人遇难。[①] 8 日,一位女警官在巴黎郊区被恐怖分子杀害。该恐怖分子还绑架了十几位人质,其中四人死亡。[②] 同年 11 月 13 日,巴黎同一天内发生了六起恐怖袭击事件,恐怖分子分别在多地进行袭击。[③] 这次事件造成了 129 人死亡,超过 350 人受

① Laura Smith-Spark, Dana Ford and Jethro Mullen, "Charlie Hebdo Attack: What We Know and Don't Know," January 21, 2015, https://edition.cnn.com/2015/01/07/europe/charlie-hebdo-attack-summary/index.html, 访问时间:2024 年 11 月 10 日。

② Josh Levs, Ed Payne and Michael Pearson, "A Timeline of the Charlie Hebdo Terror Attack," January 10, 2015, https://edition.cnn.com/2015/01/08/europe/charlie-hebdo-attack-timeline/index.html, 访问时间:2024 年 11 月 10 日。

③ France24, "November 2015 Attacks: A Timeline of the Night that Shook the French Capital," August 9, 2021, https://www.france24.com/en/france/20210908-paris-november-2015-attacks-a-timeline-of-the-night-that-shook-the-city, 访问时间: 2024 年 11 月 10 日。

伤。[①] 该袭击事件是目前为止“伊斯兰国”极端恐怖组织在欧洲造成的最大规模的恐怖袭击事件。

2015 年恐怖主义威胁的严重性使得法国的威胁形势发生重大性质的变化。这些事件也表明,法国本土并不是安全之地。11 月 13 日巴黎恐怖袭击发生后,法国宣布进入紧急状态,边境封锁、中小学停课、巴黎增派安全部队。[②] 恐怖主义袭击的伤亡后果远超以往,这改变了法国政府对于恐怖主义威胁的认识,由原本的自信变为更加重视反恐。法国总理瓦尔斯曾在 2016 年接受采访时表示,法国正在面对最大程度的恐怖主义袭击威胁。[③]

可见,法国的恐怖主义威胁发展出现了新形势,恐怖主义威胁事件类型已经从之前的重复威胁事件变为新生威胁事件。恐怖主义威胁出现新的重大变化,对于恐怖主义威胁后果的预测难度变高,威胁具有非日常性。过去所积累的关于恐怖主义的知识和信息已经难以适用于此时的情形,大众对于恐怖主义威胁的熟悉性下降。在新的情形下,恐怖主义威胁的不确定性升高,人们的恐惧感也随之升高。在 11 月法国发生恐袭的几天之后,巴黎的几个街区有大批民众陷入惊慌并四处逃跑,后经调查发现这是燃放爆竹引发的虚惊一场。巴黎民众的恐慌行为也显现出大众对恐怖主义的恐惧心理

---

① “ISIS Claims Deadly Paris Attacks, ‘First of the Storm’,” ABC News, November 15, 2015, https://abcnews.go.com/International/isis-claims-deadly-paris-attacks-storm/story?id=35201302, 访问时间:2024 年 3 月 10 日。

② 中国新闻网:《巴黎遭恐袭规模“前所未有” 奥朗德称将无情还击》,2015 年 11 月 15 日,来源:https://www.chinanews.com/gj/2015/11-15/7623710.shtml,访问时间:2024 年 10 月 3 日;中国新闻网:《法国恐袭事件致 153 人遇难 5 名袭击者可能已丧生》,2015 年 11 月 14 日,来源:https://www.chinanews.com.cn/gj/2015/11-14/7623139.shtml,访问时间:2024 年 10 月 10 日;中国新闻网:《巴黎多处遇袭已致 35 人死 奥朗德宣布紧急状态》,2015 年 11 月 14 日,来源:https://www.chinanews.com/gj/2015/11-14/7623001.shtml,访问时间:2024 年 10 月 10 日。

③ 韩冰、应强:《法总理瓦尔斯说法国仍面临最大程度恐袭威胁》,2016 年 9 月 11 日,来源:https://news.cctv.com/2016/09/11/ARTIiRSdIo8dUKAoQIADvufr160911.shtml,访问时间:2024 年 2 月 26 日。

和担忧情绪。[①] 不仅如此,由于法国只有持有射击证才能合法持枪,2015 年查理周刊事件之后,法国考取射击证的人数激增,射击俱乐部爆满。[②] 这些现象反映出法国大众对于恐怖主义恐惧感的上升。

法国大众对于恐怖主义威胁感知的上升也反映在欧洲晴雨表的调查中(见图 7)。法国民众对于恐怖主义威胁感知在 2015 年大幅度上升,在 2017 年达到顶点。大众对于恐怖主义的不安和恐惧还反映在民众对于政府安全政策的不满中。在法国失业率较高,经济问题严峻的情况下,法国民众最关心的却是安全问题。[③] 对于恐怖主义的担忧弥漫于整个法国社会。在 2019 年的一项民调中,仍有 82% 的法国民众认为未来再次出现恐袭的可能性很高。[④]

通过法国恐怖主义威胁及大众安全威胁感知变化的分析,可以看出随着恐怖主义威胁事件的不断发生,威胁事件类型演化为重复威胁事件,法国大众对于恐怖主义威胁的信息增加、知识增长,熟悉度上升,恐惧心理下降。在 2010 年至 2013 年间,虽然恐怖主义威胁有所发展,但大众威胁感知却并没有随之增长,反而出现钝化现象。当恐怖主义威胁出现重大新变化,进一步升级后,威胁事件类型转变为新生威胁事件。面对新的威胁形势,人们对于恐怖主义威胁缺少知识和信息,熟悉度下降,不确定性升高,大众对于恐怖主义威胁的感知上升。从法国大众对恐怖主义威胁感知的变化可检验假设 1 和假设 2。

---

① "'Collective Panic' in Paris after Apparent Firecrackers," CBS News, November 15, 2015, https://www.cbsnews.com/news/panic-at-scene-of-one-of-paris-attacks-after-police-storm-it/,访问时间:2024 年 9 月 2 日;"Paris Plaza Cleared of Mourners, Panic Breaks out at Other Site," November 15, 2015, https://toronto.citynews.ca/2015/11/15/paris-plaza-cleared-of-mourners-panic-breaks-out-at-other-site/,访问时间:2024 年 9 月 2 日。

② 李永群:《威胁增大,恐袭阴影笼罩法国社会》,载《人民日报》,2016 年 9 月 13 日,第 21 版。

③ 同上。

④ 刘玲玲:《法国多措并举打击恐怖主义》,载《人民日报》,2020 年 3 月 16 日,第 16 版。

六、结论

通过对美国和意大利民众对网络攻击威胁以及法国民众对于恐怖主义威胁的感知变化案例，可以看出重复威胁事件下大众安全威胁感知会出现钝化现象，而新生威胁事件下大众安全威胁感知则不钝化。随着安全威胁事件的持续发生，大众关于威胁的信息增加、知识增长以及熟悉性上升会导致威胁的不确定性下降，大众的恐惧心理下降，进而出现大众安全威胁感知钝化现象。

相比于已有关于安全威胁感知的文献，本文的推进主要体现为三点：第一，在大众安全威胁感知影响因素的分析中引入了时间因素，并说明了时间因素引起安全威胁感知钝化的具体机制，拓宽了大众安全威胁感知的研究视角。第二，说明了大众安全威胁感知钝化现象的含义、表现形式和出现原因，阐明了大众安全威胁感知长期变化规律。第三，揭示了不同安全威胁事件类型对大众安全威胁感知的影响差异，为安全威胁感知相关研究提供了更细致的分析框架。

在理解大众安全威胁感知长期变化规律的基础上，本文有助于更好地推进相关的研究。如能够考虑时间因素，并有意识关注大众安全威胁感知钝化现象，有可能为理解和预测他国大众安全威胁感知变化提供新的启发。再如，在政策分析中，如果加入关于安全威胁事件类型及大众安全威胁感知钝化的考量，有助于更好地预测政策实施和执行时的民众支持意愿。除此之外，本文的研究发现也有利于更好地认识、理解和分析气候变化、网络攻击等长期安全威胁对大众感知的影响，在此基础上将有助于理解现实和制定相关政策。