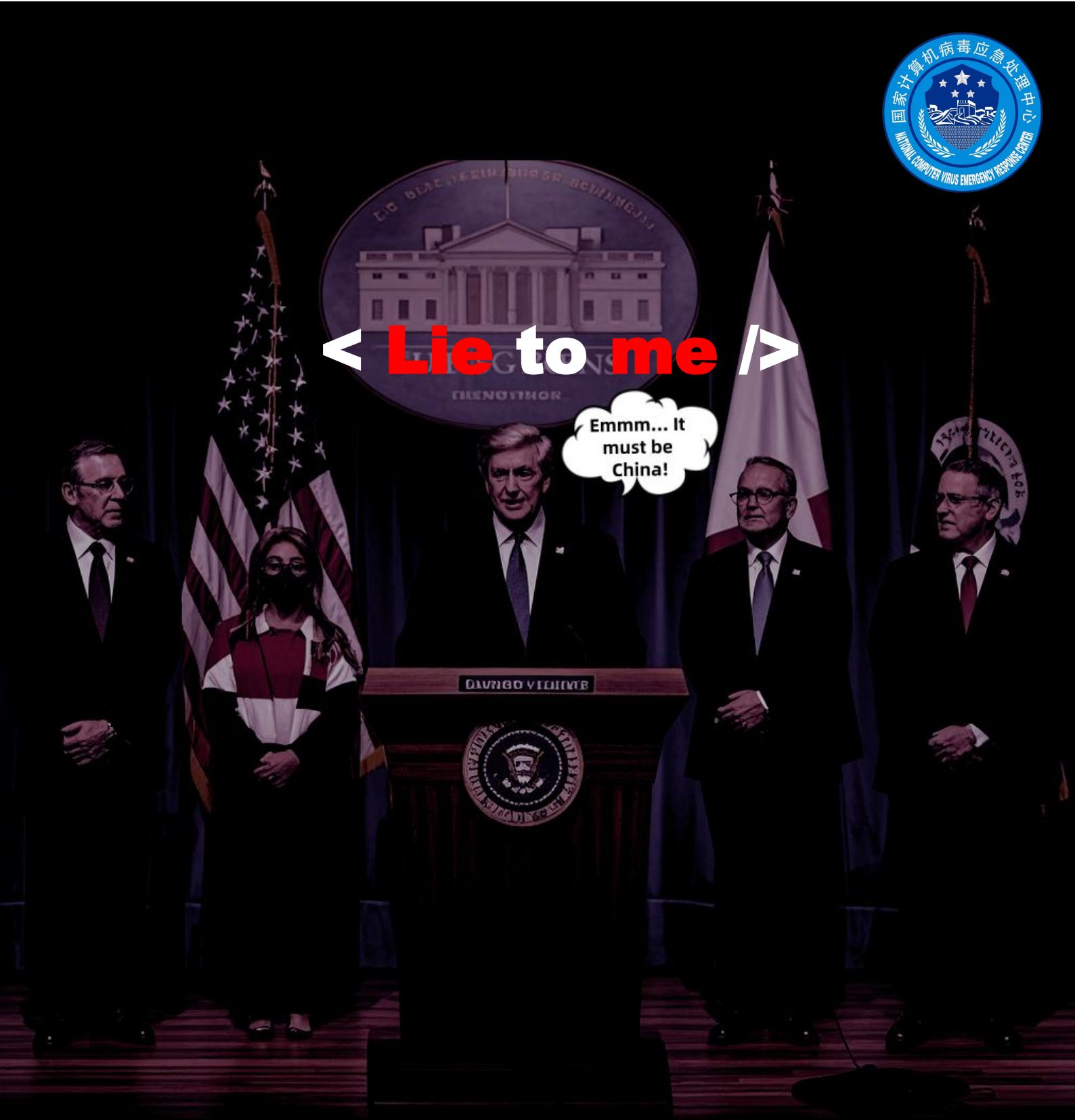


“伏特台风”III

—— 揭密美国政府机构实施的网络间谍和虚假信息行动

〔**内容摘要：**在前两篇“伏特台风”调查报告发布后，美国联邦政府机构、主流媒体和微软公司继续集体保持沉默，但以罗伯特·乔伊斯等人为代表的前任和现任美国情报机构及美国网络安全主管部门官员，部分美国网络安全企业和网络安全媒体却出来发声，竭力狡辩，但避而不谈我们在前两篇文章中公布的证据，这再次充分暴露了其“做贼心虚”“贼喊捉贼”的真实面目。本次在前两篇报告的基础上，进一步公开美国联邦政府、情报机构和“五眼联盟”国家针对中国和德国等其他国家及全球互联网用户联合实施网络间谍窃听窃密活动，并通过误导溯源归因分析的隐身“工具包”实施“假旗行动”掩盖自身恶意网络攻击行为，嫁祸他国的铁证，以及美采取“供应链”攻击，在互联网产品中植入后门，“预先埋伏”的事实，彻底揭穿“伏特台风”这场由美国联邦政府自编自导自演的政治闹剧。〕

一、引言

2024 年 4 月 15 日和 7 月 8 日，中国国家计算机病毒应急处理中心、计算机病毒防治技术国家工程实验室和 360 数字安全集团先后发布了题为《伏特台风——美国情报机构针对美国国会和纳税人的合谋欺诈行动》[1]和《伏特台风 II——揭密美国政府机构针对美国国会和纳税人的虚假信息行动》[2]的专题报告，全面

[1] https://www.cverc.org.cn/head/zhaiyao/news20240415-FTTF.htm
[2] https://www.cverc.org.cn/head/zhaiyao/news20240708-FTTFER.htm

揭露了美国政府机构为继续把持所谓“无证监视权”对全球电信和互联网用户实施无差别监听，并为背后相关利益集团攫取更大的政治利益和经济利益，架接虚构子虚乌有的中国网络攻击威胁，合谋欺诈美国国会议员和纳税人的“纸牌屋”式闹剧。报告发布后，谎言制造者、美国“环球媒体署”及其操弄的美西方主流媒体一如既往地保持沉默，但这种“沉默”还是在国际社会引发广泛关注。先后有来自美国、欧洲、亚洲等国家和地区的50余位网络安全专家通过各种方式与我中心联系，认为美国和微软公司将“伏特台风”与中国政府关联，缺乏有效证据，同时表达了对美国操弄“伏特台风”虚假叙事的关切。同时，互联网上相关话题热度持续上升也让国际社会更加清晰地认识美国及其网络霸权的真实面目，认清美国利用互联网无差别监听全球的现实危害。为此，我们有必要公开更多美国政府机构编造“伏特台风”虚假叙事，组织实施“假旗”行动，以及对中国发动网络攻击的客观证据，继续深入揭露美国“贼喊捉贼”和“掩耳盗铃”的把戏。

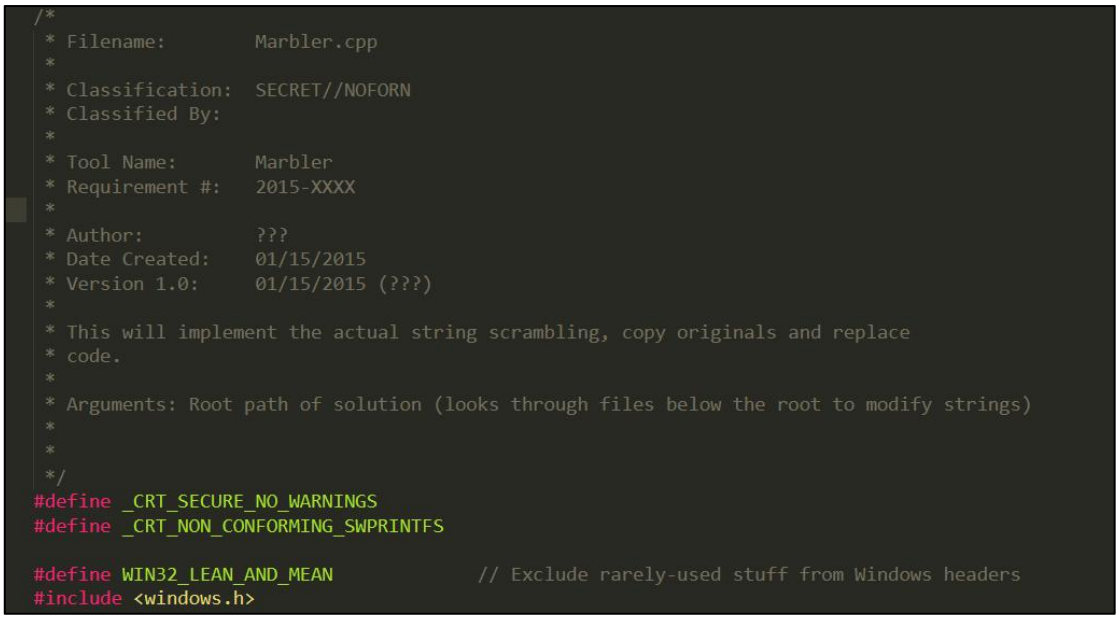
二、网络空间的“变色龙”

众所周知，美国是全球最大的军火供应商，规模庞大的军事工业体系、强大的军工复合体已经成为左右美国政治、经济、军事政策的重要基石，由此形成的美国网络武器库不仅规模庞大、形式多样，而且功能复杂、产品丰富。此前，中国国家计算机病

毒应急处理中心已经连续公开披露了多款美国国家安全局（NSA）、中央情报局（CIA）开发的网络武器，并在《中国西北工业大学遭到美国NSA网络攻击事件调查报告》中，详细分析了相关美国情报机构在对外网络攻击中所用的多款网络武器的功能，以及采用的高隐蔽性攻击技战术，但这些显然只是美国“黑客帝国”庞大网络武器库的“冰山一角”。

长期以来，美国在网络空间积极推行“防御前置”战略并实施“前出狩猎”战术行动，也就是在对手国家周边地区部署网络战部队，对这些国家的网上目标进行抵近侦察和网络渗透。为适应这种战术需要，美国情报机构专门研发了用于掩盖自身恶意网络攻击行为、嫁祸他国并误导溯源归因分析的隐身“工具包”，代号“大理石”（Marble）。该工具包是一个工具框架，可以与其它网络武器开发项目集成，辅助网络武器开发者对程序代码中各种可识别特征进行“混淆”，有效“擦除”网络武器开发者的“指纹”，类似于改变了“枪械”武器的“膛线”，转移武器的指向，使调查人员无法从技术角度追溯武器的真实来源。此外，该框架还具有一个更加“无耻”的功能，就是可以随意插入中文、俄文、朝鲜文、波斯文、阿拉伯文等其他语种的字符串，这显然是为了误导调查人员，并栽赃陷害中国、俄罗斯、朝鲜、伊朗以及众多的阿拉伯国家。

据“大理石”工具框架源代码及其注释显示（如图 1 所示），它被确定为一个机密级（且不可向国外透露）的武器研发计划，起始时间不晚于 2015 年。显然，该计划是美国情报机构为自身量身打造的“秘密武器”，甚至严禁透露给所谓的“盟友”国家。



```
/*
 * Filename:        Marbler.cpp
 *
 * Classification:  SECRET//NOFORN
 * Classified By:
 *
 * Tool Name:       Marbler
 * Requirement #:   2015-XXXX
 *
 * Author:          ???
 * Date Created:    01/15/2015
 * Version 1.0:     01/15/2015 (???)
 *
 * This will implement the actual string scrambling, copy originals and replace
 * code.
 *
 * Arguments: Root path of solution (looks through files below the root to modify strings)
 *
 *
 */
#define _CRT_SECURE_NO_WARNINGS
#define _CRT_NON_CONFORMING_SWPRINTFS

#define WIN32_LEAN_AND_MEAN             // Exclude rarely-used stuff from Windows headers
#include <windows.h>
```

图 1 “大理石”计划源代码

“大理石”工具框架可以使用超过 100 种混淆算法，将源代码文件中可读的变量名、字符串等替换为不可读（不可识别）内容，并且可以插入特定的干扰字符串。如图 2、图 3、图 4 和图 5 所示。

```
virtual int ScrambleW(wchar_t *wcToScramble, unsigned int iNumOfChars) = 0;

/*
    Args:
        cToScramble[in]: is the buffer containing a char string to scramble
        iNumOfChars[in]: the number of CHARs in the buffer

        Ret: > 0 == SUCCESS,  <=0 == FAILURE
*/
virtual int ScrambleA(char *cToScramble, unsigned int NumOfChars) = 0;


/*
    Args:
        cVarName[in]: the name of the variable being replaced
        cStringLiteral[in]: the string literal to be added to the insert (after scrambling)
        iNumOfChars[in]: the number of characters in the buffer
        cInsert[out]: the insert to replace CARBLE\BARBLE declaration in the c/cpp file

        Ret: > 0 == SUCCESS,  <=0 == FAILURE
*/
```

图 2 混淆函数

```
#include "IScramble.h"

//--------------C Algorithms----------------------------
#include "MBL_FORLOOP_XOR1.h"
#include "MBL_FORLOOP_XOR2.h"
#include "MBL_FORLOOP_XOR3.h"
#include "MBL_FORLOOP_XOR4.h"

#include "MBL_FORLOOP_FUNC_XOR1.h"
#include "MBL_FORLOOP_FUNC_XOR2.h"
#include "MBL_FORLOOP_FUNC_XOR3.h"
#include "MBL_FORLOOP_FUNC_XOR4.h"
#include "MBL_FORLOOP_FUNC_XOR5.h"
#include "MBL_FORLOOP_FUNC_XOR6.h"



#include "MBL_FORLOOP_RXOR1.h"
#include "MBL_FORLOOP_RXOR2.h"
#include "MBL_FORLOOP_RXOR3.h"
#include "MBL_FORLOOP_RXOR4.h"

#include "MBL_FORLOOP_FUNC_RXOR1.h"
#include "MBL_FORLOOP_FUNC_RXOR2.h"
#include "MBL_FORLOOP_FUNC_RXOR3.h"
#include "MBL_FORLOOP_FUNC_RXOR4.h"
```

图 3 混淆算法

```
        {
            if (bHasBackSlash)
                wsprintf(pszFullPath, L"%s%s", pszRoot, FindFileData.cFileName);
            else
                wsprintf(pszFullPath, L"%s\\%s", pszRoot, FindFileData.cFileName);

            //Process File
            if (PathMatchSpec(pszFullPath, L"*.c") || PathMatchSpec(pszFullPath, L"*.cpp") || PathMatchSpec(pszFullPath, L"*.h"))
            {
                if (!PathMatchSpec(FindFileData.cFileName, L"Marble.*"))
                {
                    BOOL bProcessed = ProcessFile(pszFullPath, pMarblerList);

                    //Global Flag for error
                    if (!bProcessed)
                    {
                        g_bModificationError = TRUE;
                        wprintf(L"Error modifying file\n");
                    }
                }
```

图 4 文件处理功能函数

```
if (pNode->eStringType == stCHAR)
{
    int iResult = g_pScram->ScrambleA((CHAR *)lpbLine, iLineLen);
    if (iResult > 0)
    {
        if (VerifyScramRatio(pNode->eStringType, (LPBYTE)pNode->cString, lpbLine, iLineLen))
        {
            iResult = g_pScram->CreateStringLiteralA(lpbLine, iLineLen, cLiteral);
            if (iResult > 0)
            {
                iResult = g_pScram->GenerateInsertA(cVarName, cLiteral, iLineLen, cInsert);
                if (iResult <= 0)
                    bModError = TRUE;
            }
            else
                bModError = TRUE;
        }
        else bModError = TRUE;
    }
    else
        bModError = TRUE;
}
else
{
    int iResult = g_pScram->ScrambleW((WCHAR *)lpbLine, iLineLen);
    if (iResult > 0)
    {
        if (VerifyScramRatio(pNode->eStringType, (LPBYTE)pNode->cString, lpbLine, iLineLen))
        {
            iResult = g_pScram->CreateStringLiteralW((WCHAR *)lpbLine, iLineLen, cLiteral);
            if (iResult > 0)
            {
                g_pScram->GenerateInsertW(cVarName, cLiteral, iLineLen, cInsert);
                if (iResult <= 0)
                    bModError = TRUE;
            }
```

图 5 文件处理功能函数（续）

我们甚至可以从“大理石”的测试实例源代码中找出被刻意插入的“外语”字符串，而所谓的“外语”仅包括阿拉伯文、中文、俄文、朝鲜文和波斯文（如图 6 所示）。

```
//Add foreign languages
//Arabic
WARBLE wcArabic[] = L" آلم أديه عيطق ٣٠يف ءادزلود م شل الك ل عنلش ا جمل جمت عو علاّت ثويح غ انوض ل ال قش ل انيبتس ىل
sb.Append((LPBYTE)wcArabic, 380);


//Chinese
WARBLE wcChinese[] = L"洴洀兆 墄煓瑜 鹿楁榍 詃 鑐鑏, 篙黫齜 逯郹頎峳滤 潭滤湤 麐 踶輵 洋絜溄 螭蜹謕 崞愊憷 榏 趏跮, 嵘 垡婖 蟷螺蝥 鍴
sb.Append((LPBYTE)wcChinese, 266);


//Russian
WARBLE wcRussian[] = L"Зыд нэ нонюмэш контынтёонэж. Видэ бландит ан квуй, дуо декам эпикюре эа. Йн дйкит мольлиз дэлььякатезш
sb.Append((LPBYTE)wcRussian, 550);


//Korean
WARBLE wcKorean[] = L"사용할 수있는 구절 많은 변화가 있지만, 대부분의, 주입 유머로, 어떤 형태의 변경을 입었거나 조금이라도 믿을 보이지
sb.Append((LPBYTE)wcKorean, 288);

//Farsi
WARBLE wcFarsi[] = L" لورم ايپسوم ك طحنلم ( باان گلیس Lorem ipsum) به م تنیآزلم ی شکو ردینعمیب پ چت عص مخصآر
sb.Append((LPBYTE)wcFarsi, 1710);

lpbData = (LPBYTE)malloc(sb.GetUsedSize());
dwDataLen = sb.GetUsedSize();
memcpy(lpbData, sb.GetBufferAddress(), sb.GetUsedSize());

return;
```

图 6 在文件中插入“外语”

“大理石”工具包框架充分暴露了美国情报机构在全世界开展的无差别、无底线网络间谍活动，并实施“假旗”（False Flag）行动，以误导调查人员和研究人员，并实现栽赃“对手国家”的阴谋。

这种“假旗”行动并不仅限于代码特征层面，通过巧妙模仿网络犯罪团伙的攻击技战术，美国情报机构还可以虚构出各类完美的“口袋”组织，这一点我们已经在第二份报告中进行了阐述。因此，美国网络战部队和情报机构的黑客就如同变色龙一般在网络空间中任意变换身份、变更形象，“代表”其他国家在全球实施网络攻击窃密活动，并将脏水泼向美国的非“盟友”国家。

据可靠渠道透露，“假旗”（False Flag）行动实际上是美国情报机构“影响力行动”（英国称为“线上掩护行动”）的重要组成部分。美国和“五眼联盟”国家的秘密文件显示，“影响力行动”主要包括两个方面，即“虚假信息行动”和“技术干扰行动”，美国国家安全局（NSA）对于“技术干扰行动”专门编写了《实施手册》，而其中“假旗”（False Flag）行动就是“技术干扰行动”的重要组成部分。与此同时，美国和“五眼联盟”国家的内部文件中也明确指出，实施这种“影响力行动”必须遵守四个主要原则（“4D”原则），即“否认”、“干扰”、“抹黑”和“欺骗”。而这四条主要原则恰恰覆盖了“伏特台风”行

动的全部核心要素（如图 7，图 8 所示）。

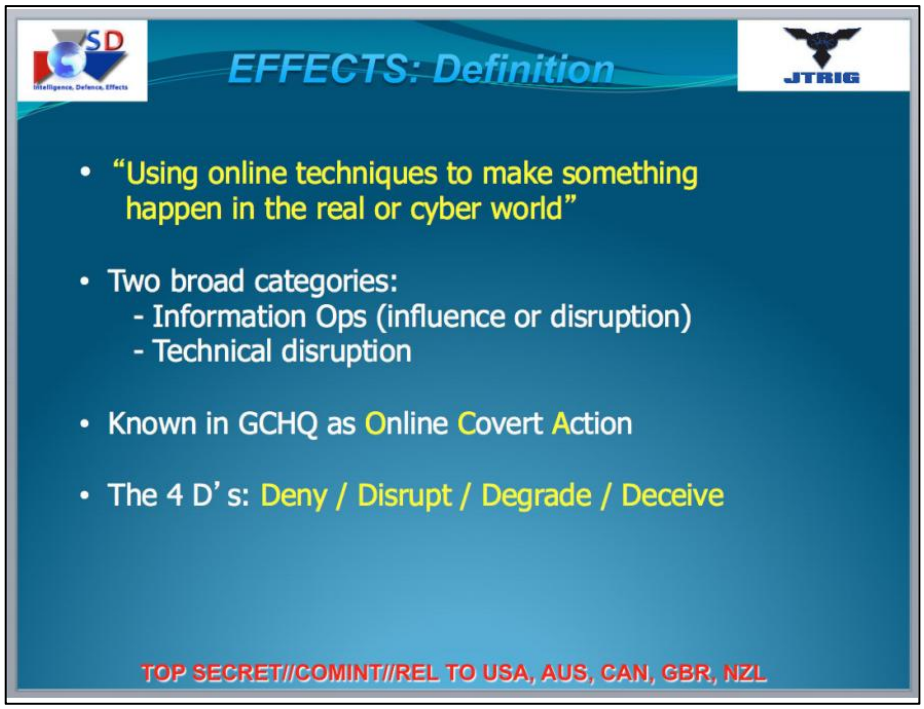


图 7 美国和五眼联盟国家对“影响力行动”的定义

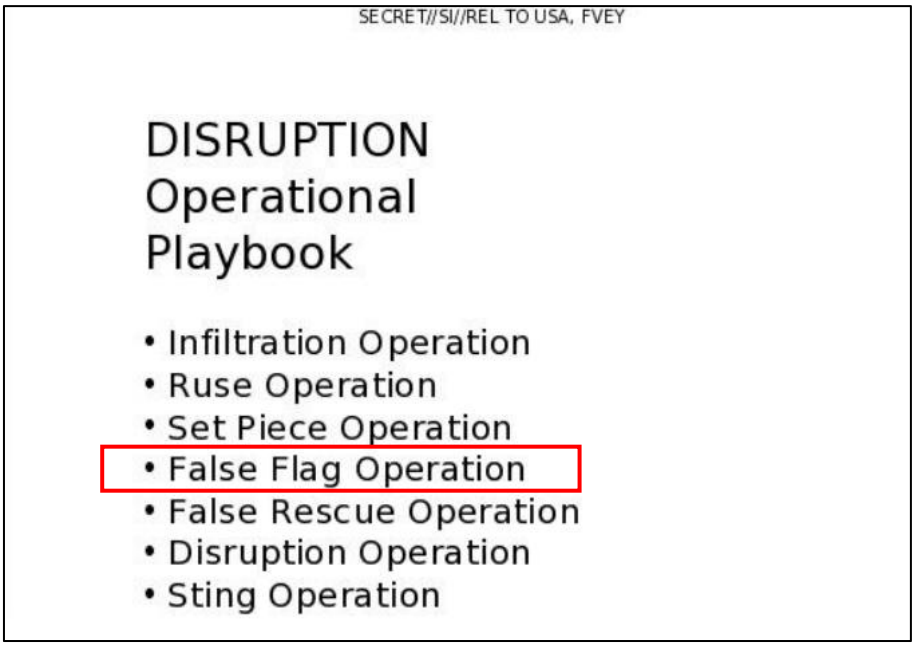


图 8 美国和五眼联盟国家关于“技术干扰行动”的实施手册

从上述证据中可以推定，“伏特台风”行动就是一个典型的、

精心设计的、符合美国资本集团利益的虚假信息行动（也就是所谓的“假旗”行动），其技战术与美国和“五眼联盟”国家情报机构在“影响力行动”中采用技战术完全吻合。而要想识破这种由美国国家级情报机构精心设计的骗局当然非常困难，由于存在大量干扰信息，仅仅依靠技术分析是远远不够的，必须综合分析多方信息和相关材料，才能发现美国情报部门不经意间暴露出来的疏忽和错误，才能正确理解和解读美国国家安全局（NSA）和中央情报局（CIA）等情报机构炮制的险恶计划。这些内容就是我们在前两份调查报告中所做的工作（参见《“伏特台风”——美国情报机构针对美国国会和纳税人的合谋欺诈行动》和《“伏特台风”II——揭密美国政府机构针对美国国会和纳税人的虚假信息行动》）。

三、网络空间的“窥探者”

在第二份报告中，我们揭露了美国联邦政府机构特别是其情报机构，为了继续把持《涉外情报监视法案》第 702 条款所赋予的“无证”监视权，不惜编造所谓外部网络威胁，发动虚假信息行动，以维持其庞大“无差别”、“无底线”监听计划的政治丑闻。本报告中，我们将进一步揭露上述“三无”监听计划的具体情况。

（一）扼住互联网的“咽喉”

据美国国家安全局（NSA）的内部绝密级资料显示（如图 9 所示），美国依托其在互联网布局建设中先天掌握的技术优势和地理位置优势，牢牢把持全球最重要的大西洋海底光缆和太平洋海底光缆等互联网“咽喉要道”，先后建立了 7 个国家级的全流量监听站，与美国联邦调查局（FBI）和英国国家网络安全中心（NCSC）紧密合作，对光缆中传输的全量数据深度开展协议解析和数据窃取，实现对全球互联网用户的无差别监听。

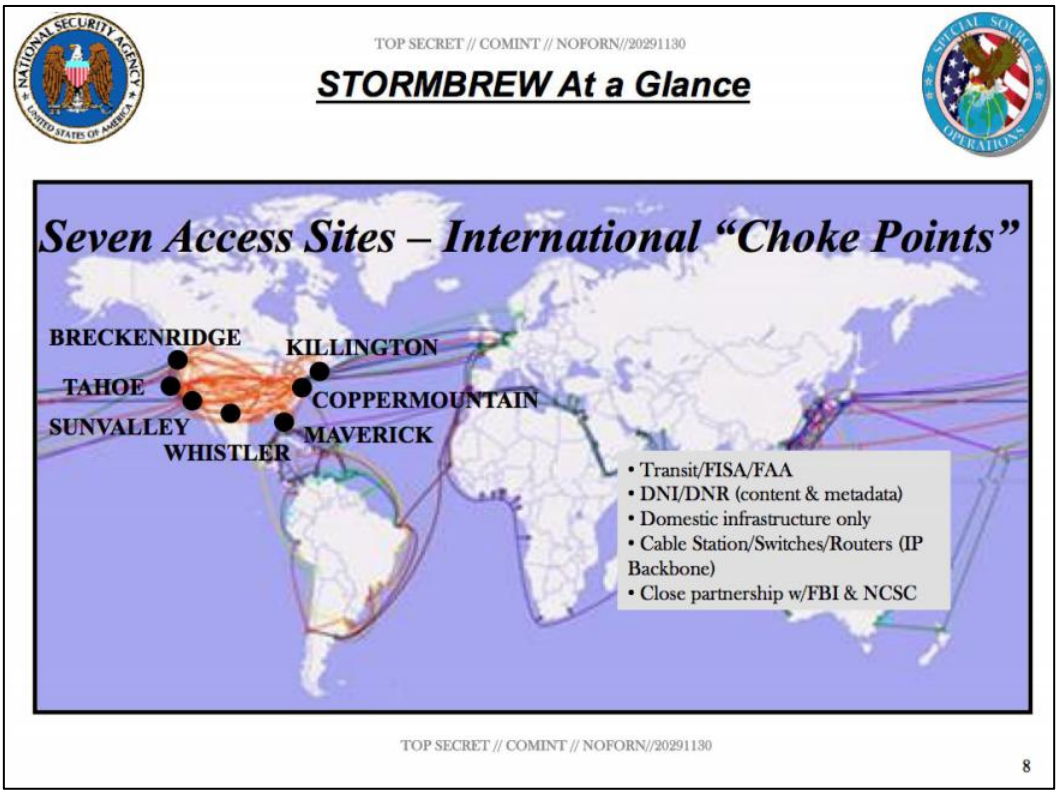


图 9 美国国家安全局（NSA）建立运营的海底光缆监听站

这些互联网数据监听和信号情报的受益者众多，除了美国联邦政府情报机构和军事机构外，还有大量美国联邦政府行政部门，包括白宫、内阁官员、美国驻外大使馆、美国贸易代表办公室、

美国国会，以及美国国务院、农业部、司法部、财政部、能源部、商务部、国土安全部等等。这就是我们在第二篇报告中所指出的，“伏特台风”计划的参与者不仅仅限于美国情报机构，而是为了服务所谓美国资本的共同利益，很多美国政府机构都在其中起到了推波助澜作用（如图 10 所示）。

图 10 美国国家安全局（NSA）情报的“客户”列表

（二）控制互联网数据的“水库”

情报监听的输出结果必然是各种可读的信息和数据，因此把海底光缆中的传输流量实时转化、翻译成可阅读、可检索的情报信息是美国国家安全局（NSA）的另一项重要工作，而在加密网

络流量占比越来越高的趋势下，这项工作也面临着巨大的挑战。为解决这个问题，美国国家安全局（NSA）实施了两个重点工程项目：**一是“上游”（UpStream）项目**，主要功能是将前述监听站拦截的海底光缆原始通信数据进行全量留存，形成规模庞大的数据“水库”，“水库”中的海量原始数据就是后续情报处理工作流程的“上游”。值得注意的是，就在刚刚结束的联合国大会期间，美国纠集部分盟友发表联合声明，宣称要维护海底光缆的安全可靠；**二是“棱镜”（Prism）项目**，其主要功能一方面是将“上游”项目中的原始通信数据按照互联网应用进行分类，并对通信内容进行还原分析；另一方面，为有效解决“上游”项目中的加密数据破解和网络通信流量路径覆盖不全等突出问题，美国政府强制规定“棱镜”项目直接从美国各大互联网企业的服务器上获取用户数据，这些互联网企业包括微软、雅虎、谷歌、脸书（现已改名为 Meta）、苹果等。而上述两个项目都是在《涉外情报监视法案》（FISA）第 702 条款的授权下建设实施的，第 702 条款成为美国情报机构代表美国联邦政府合法、公开、持续窃取全球互联网链路数据的官方依据，也成为美国戴牢“窃密帝国”高帽的扎实证据，且无法抵赖（如图 11 所示）。

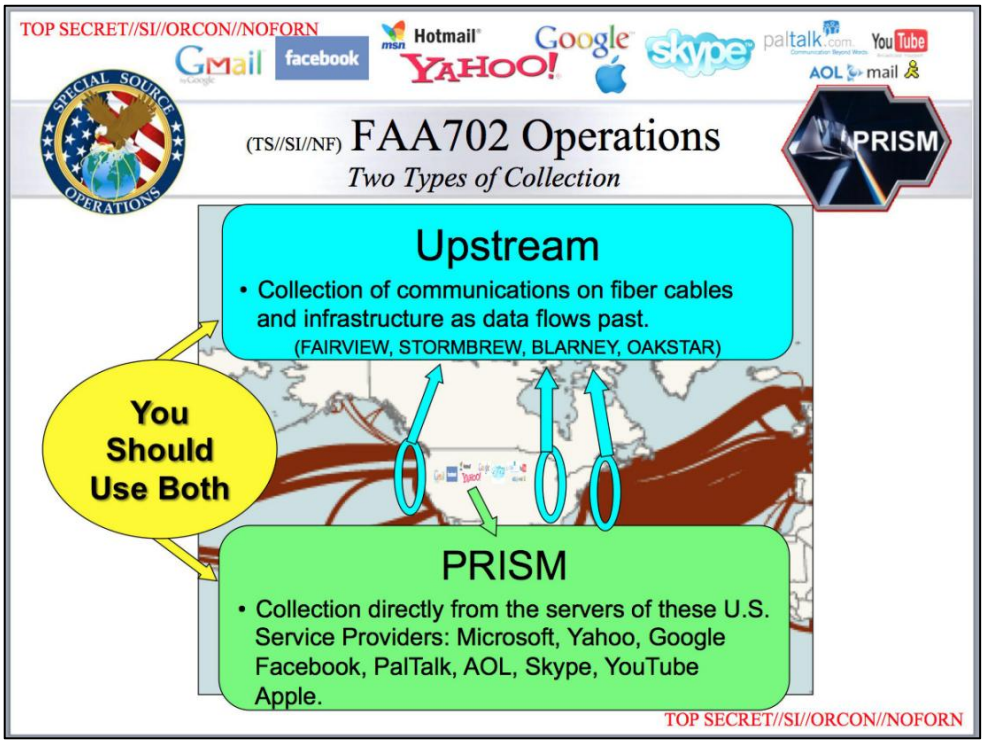


图 11 美国国家安全局（NSA）实施全球互联网监听的两大重点工程项目

（三）潜入互联网数据的“源头”

尽管美国国家安全局（NSA）已经在全球互联网上部署了规模庞大的监听系统，但如果这些系统的监听目标及其网络通信内容仅仅停留在海底光缆所覆盖的特定区域，那么这些监听系统所窃取的数据就远远不能满足美国国家安全局（NSA）的情报工作需要。为解决以上问题，美国国家安全局（NSA）针对位于监听系统“盲区”的特定目标实施了网络秘密入侵行动（CNE），而美国国家安全局（NSA）“臭名昭著”的“特定入侵行动办公室”（TAO）就是下场来干这个“脏活”的。从美国国家安全局（NSA）的绝密文件中我们可以看到，隶属于美国国家安全局（NSA）的

“特定入侵行动办公室”（TAO）在全球范围内发动无差别的网络秘密入侵行动（CNE），并植入了超过5万个间谍程序（Implants），受害目标主要集中在亚洲地区、东欧地区、非洲地区、中东地区和南美地区。我们从美国国家安全局（NSA）的内部文件中可以清楚看到，中国境内的主要城市几乎都在其网络秘密入侵行动（CNE）范围内，大量的互联网资产已经遭到入侵，这其中当然也包括西北工业大学和武汉市地震监测中心所在地区。上述间谍软件程序的命令控制中心很多都位于美国本土之外的军事基地，包括一大批位于日本、韩国、**关岛**和夏威夷的美军基地。“**关岛**”这个名字，对于阅读关注过我们前两篇报告的读者来说应该并不陌生，它可以被称为是美国政府编造传播所谓“伏特台风”谎言的最初策源地，它也将因为“伏特台风”虚假叙事而永载网络安全发展史册。而实际上，“**关岛**”美军基地根本不是什么“伏特台风”网络攻击的受害者，恰恰相反，而是大量针对中国和诸多东南亚国家网络攻击的发起者和被窃取数据的回传中心（如图12、13所示）。

对于其他国家的一些防范等级高且入侵难度大的高价值目标，美国国家安全局（NSA）的“特别入侵行动办公室”（TAO）会直接采取“供应链”攻击的方式，依靠美国在先进网络安全技术和产品方面的优势，在美国大型互联网企业或设备供应商的配

合下，从寄递物流渠道拦截攻击目标或为攻击目标提供网络接入服务的运营商所采购的美国网络设备产品，对设备进行拆解并植入后门后再重新打包发货给攻击目标。这种方式通常被使用在对他国电信和网络运营商的攻击活动中，可实现对目标电信网络运营商话单计费等系统的入侵控制，进而实现对目标人员手机通信内容的监听。在西北工业大学遭美国国家安全局（NSA）“特别入侵行动办公室”（TAO）网络攻击事件中，位于中国境内的相关电信网络运营商就遭到了这种攻击，攻击目标的通话内容，上网活动记录和现实活动轨迹都被美国国家安全局（NSA）“特别入侵行动办公室”（TAO）实时窃取（如图 14 所示）。

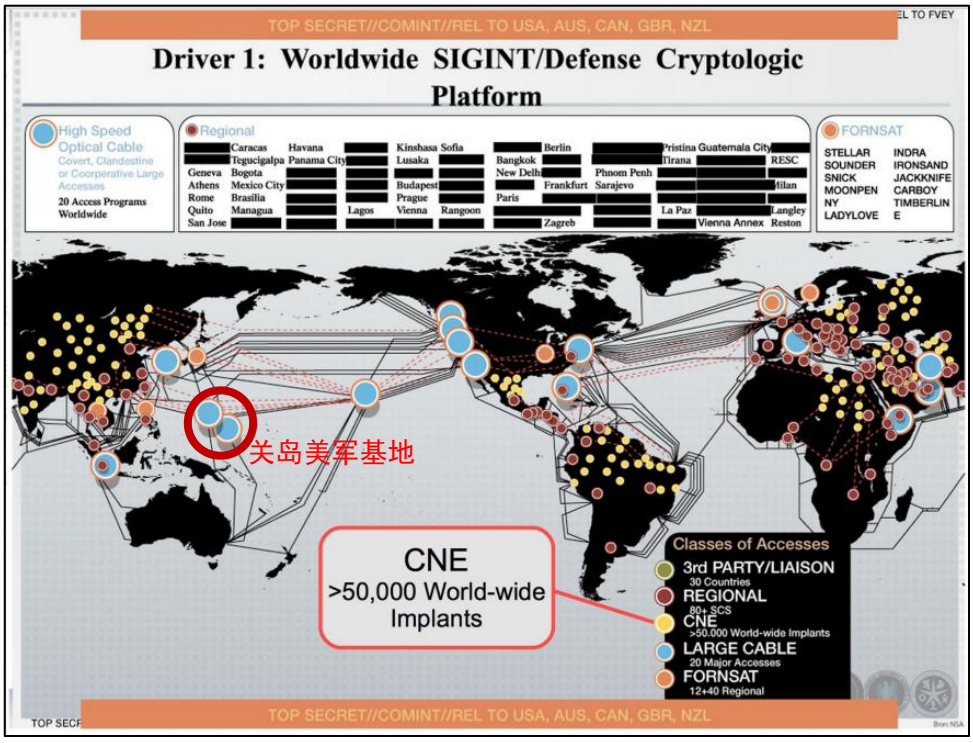


图 12 美国国家安全局（NSA）“特别入侵行动办公室”（TAO）的全球网络入侵行动示意图

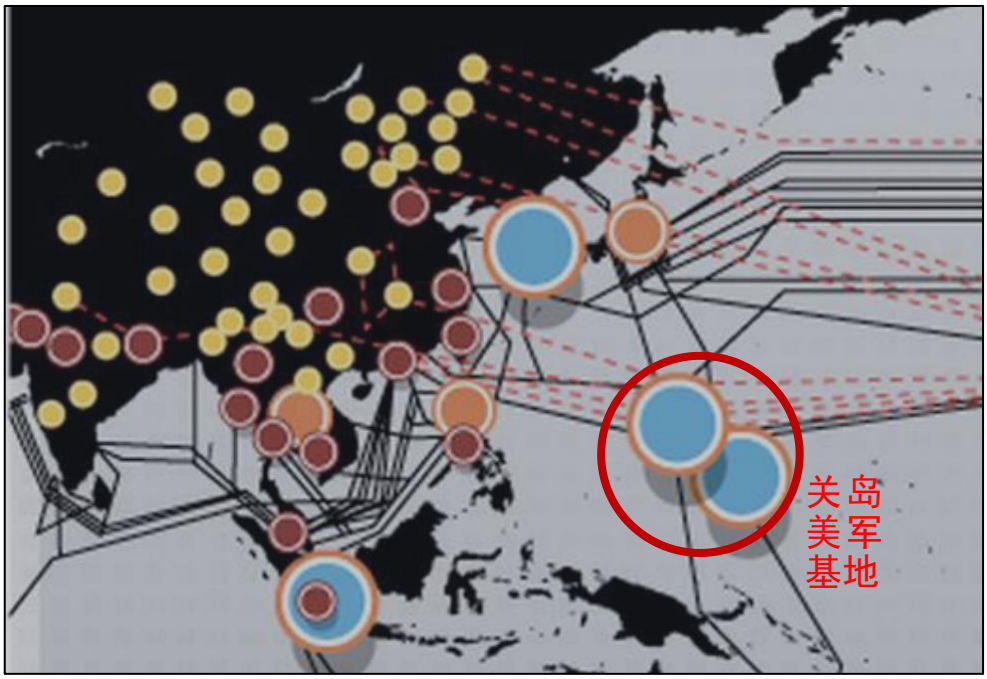


图 13 美国国家安全局（NSA）“特别行动办公室”（TAO）对中国网络实施入侵的示意图

(TS//SI//NF) Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A “load station” implants a beacon

图 14 美国国家安全局（NSA）“特别行动办公室”（TAO）技术人员正在拆开监听目标购买的美国思科公司生产的网络设备并植入后门

具有讽刺意味的是，美国国家安全局（NSA）在介绍这种供应链攻击时，使用了“pre-position”，即“预先埋伏”这一战术

词汇，该词汇特指在监听目标使用的互联网产品中预设“后门”病毒，为美国国家安全局的后续攻击控制和窃密活动埋下伏笔。我们发现，“预先埋伏”这一词汇也被美国联邦政府机构用来描述所谓的“伏特台风”组织对设在关岛等地的美国“关键基础设施”实施网络攻击时使用的战术。那么，到底是谁在遍布全球的关键基础设施中“预先埋伏”了呢？事实已经非常清楚。

（四）互联网情报的“予取予求”

通过702条款的授权，美国情报机构建立了规模庞大的全球化互联网监听网络，向美国政府机构提供了大量高价值情报，使美国政府屡屡在外交、军事、经济、科技等领域占得先机，702条款以及与之相配套的互联网监听系统成为现阶段美国维持其霸权地位的“秘密武器”。坐拥这种巨大的先发技术优势，美国联邦政府及其情报机构愈发无所顾忌，任何目标都有可能被列入“重点监控名单”，对此我们做了简要梳理，用事实说话。

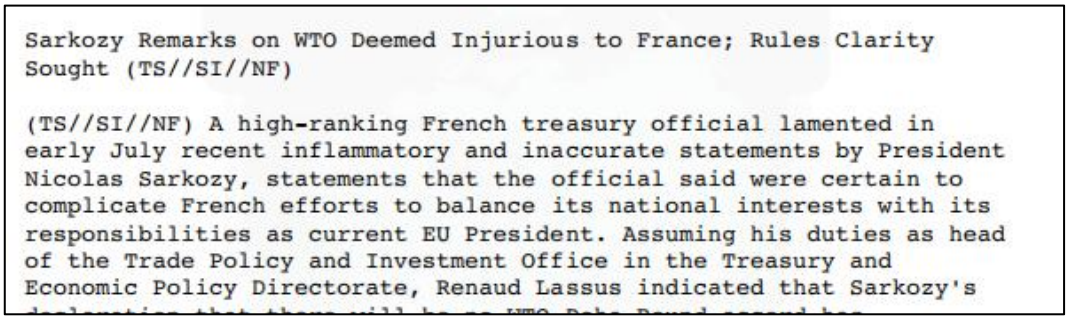
1、法国

在2004年至2012年期间，美国对法国实施了长期的间谍行动，监听内容涉及法国政府政策、外交、金融、国际交流、基础设施建设、商业和贸易活动等，其中一些重要情报被美国授权与“五眼联盟”伙伴国家共享，揭示了“五眼联盟”国家亦为美国间谍行动的获益者。美国在涉及法国间谍行动的监听记录中，既

包含法国核心的政治和经济部门电话，也包含了法国总统官邸的电话。公开曝光的美国情报部门机密文件中，含有多份通过监听法国政府高级官员对话和通讯内容而窃取的绝密情报摘要，监听对象包括前法国总统（如图 15 所示）、法国财政部长、法国外交部长、法国参议员、法国财政和经济政策局官员、法国驻美国大使，以及直接负责欧盟贸易政策的官员等。

情报内容涉及法国政府对世界贸易组织（World Trade Organization）、跨太平洋伙伴关系协定（Trans-Pacific Partnership Agreement）、七国集团（G7）和二十国集团（G20）的相关政策和内部考虑，以及法国财政预算、法国汽车业衰落以及法国公司参与伊拉克“石油换食品”（Oil-for-Food）计划的情况等。

美国在执行上述行动的经济间谍命令中，明确要求收集法国所有与电信、电力、天然气、石油、核能和可再生能源，以及环境和医疗技术相关的重大项目的销售和融资信息，并要求拦截（窃取）每一笔价值超过 2 亿美元的法国公司合同或交易，直接影响法国巴黎银行（BNP Paribas）、安盛（AXA）和法国农业信贷银行、标致（Peugeot）和雷诺（Renault）、道达尔（Total）和奥兰治（Orange）等法国大型企业，同时还影响到法国主要的农业协会。美国国家安全局（NSA）在针对法国的间谍行动中窃取掌握的部分情报内容摘要如表 1 所示。



Sarkozy Remarks on WTO Deemed Injurious to France; Rules Clarity Sought (TS//SI//NF)

(TS//SI//NF) A high-ranking French treasury official lamented in early July recent inflammatory and inaccurate statements by President Nicolas Sarkozy, statements that the official said were certain to complicate French efforts to balance its national interests with its responsibilities as current EU President. Assuming his duties as head of the Trade Policy and Investment Office in the Treasury and Economic Policy Directorate, Renaud Lassus indicated that Sarkozy's

图 15 美国国家安全局（NSA）针对前法国总统萨科齐的监听记录

表 1 美国国家安全局（NSA）针对法国时任政府官员的部分情报监听记录

日期	情报类别	情报内容
2004 年	法国驻华盛顿大使情报	法国驻华盛顿大使计划公布据称从 Oil-for-Food（OFF）计划中获利的美国公司名单。
2006 年	法国政府高层通信情报	法国时任总统希拉克和法国外交部长讨论联合国任命相关事宜。
2008 年	法国政府高层通信情报	法国财政和经济政策局长对于法国时任总统萨科齐关于世贸组织谈判协议可能对法国产生负面影响的言论感到不满。
2008 年	法国政府高层通信情报	法国时任总统萨科齐将世界经济危机归咎于美国政府，表示法国将带头追求世界金融体系的变革。
2010 年 3 月 24 日	法国政府高层通信情报	法国驻华盛顿大使和法国总统的外交顾问之间的交流对话：法国时任总统萨科齐计划在 2010 年 3 月 31 日与美国时任总统奥巴马在华盛顿会晤时提出一些敏感话题，涉及美国退出双边情报合作协议（该协议可能会限制美国继续监视法国的能力）、法国可能承诺向阿富汗提供军事训练人员，欧洲航空防务与航天公司（EADS）可能与美国军方签订加油机合同，以及与法国烈酒公司保乐力加（Pernod Ricard）有关的商标纠纷等。
2011 年 6 月 10 日	法国政府高层通信情报	法国时任总统萨科齐和法国外交部长的谈话内容：萨科齐对以色列和巴勒斯坦问题发表强硬言论。
2011 年 8 月 2 日	法国政府高层通信情报	驻华盛顿的法国和欧盟官员之间的谈话：强烈批评美国贸易政策，称 TPP（跨太平洋伙伴关系协定）是针对中国的对抗。

日期	情报类别	情报内容
2012 年 5 月 22 日	法国政府高层通信情报	法国政府内部对持续的欧元区危机对法国利益和法国企业的影响感到担忧，尤其是希腊退出欧元区的问题。法国时任总统奥朗德对德国时任总理默克尔在危机问题上的不妥协态度表示不满，同意在默克尔不知情的情况下，在法国官员和德国反对党成员之间举行秘密会议，讨论危机。
2012 年 7 月 31 日	法国政府高层通信情报	法国财政部长和法国参议员的对话：法国财政部长表示，法国经济陷入困境，预计未来两年将非常糟糕。
2012 年	美国针对法国的间谍命令	要求对法国进行长期的经济间谍活动，以获取有关法国公司经济活动的细节以及法国政府的经济政策和决定。涉及法国与美国、其他国家和国际机构的经济关系，法国的金融和贸易政策，以及法国对八国集团（G8）和二十国（G20）集团议程的看法等。
2012 年	美国针对法国的经济间谍令	指示美国间谍收集法国所有与电信、发电、天然气、石油、核能和可再生能源以及环境和医疗技术相关的重大项目的销售和融资信息。同时要求拦截和上报所有价值超过 2 亿美元的法国公司合同和谈判。相关情报将被报送至美国各贸易、政治和情报机构。
2012 年	法国政府官员会议议程情报	法国财政部为经济、财政和工业部长起草了用于 G7 和 G20 会议的谈话要点，包括敦促美国银行业改革、计划支持美国关于战略石油储备的倡议等。

2、德国

美国国家安全局（NSA）的机密文件显示，尽管德国联邦情报局（BND）和德国联邦宪法保卫局（BfV）等情报机构多次主动配合美国情报机构开展对欧洲地区甚至德国本土开展监听活

动[3]，甚至还曾与美国中央情报局（CIA）合伙收购和经营位于瑞士的加密技术公司 Crypto AG，从而向监听目标提供带有后门的加密产品[4]。但美国还是把德国排除在“五眼联盟”之外，并划为第三等级的伙伴，也就是说既是利益伙伴，也是监视目标，充满了不信任。

实际上，美国陆军、空军、海军以及美国国家安全局在德国建立了大量秘密情报站，用于监视德国和其他欧洲国家（如图 16 所示）。

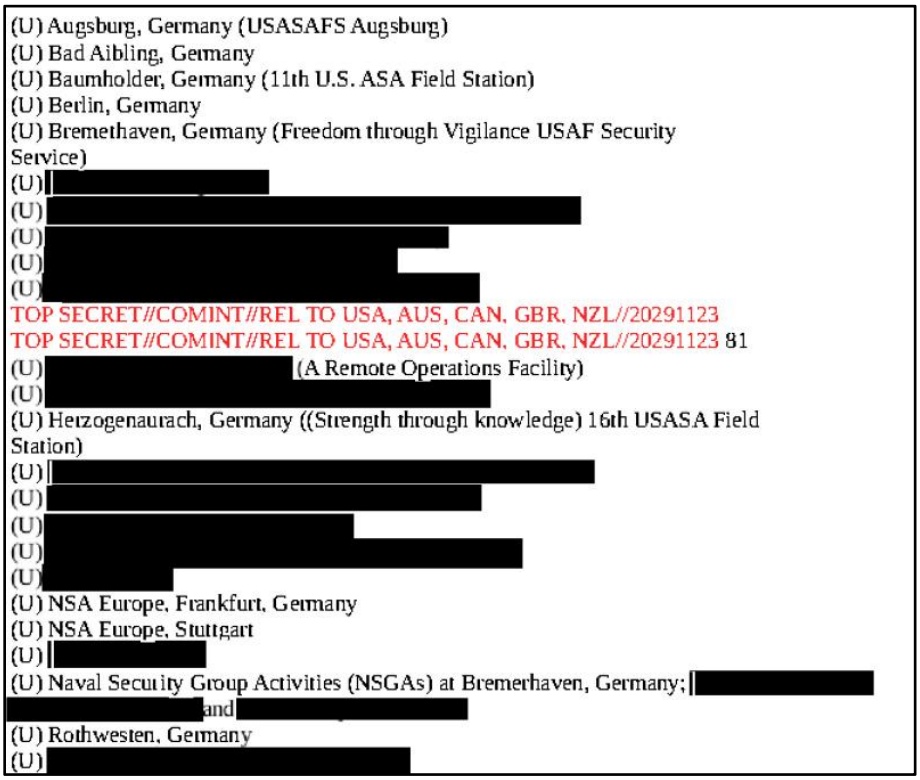
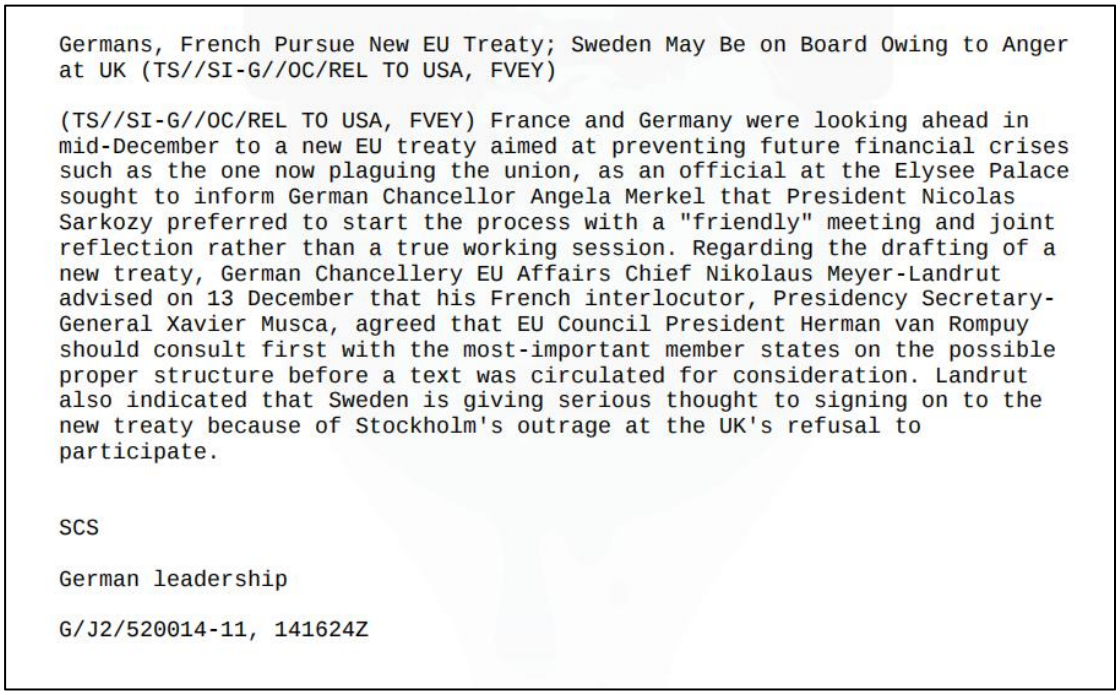

(U) Augsburg, Germany (USASAFS Augsburg)
(U) Bad Aibling, Germany
(U) Baumholder, Germany (11th U.S. ASA Field Station)
(U) Berlin, Germany
(U) Bremethaven, Germany (Freedom through Vigilance USAF Security Service)
(U) [redacted]
(U) [redacted]
(U) [redacted]
(U) [redacted]
(U) [redacted]
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20291123
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20291123 81
(U) [redacted] (A Remote Operations Facility)
(U) [redacted]
(U) Herzogenaurach, Germany ((Strength through knowledge) 16th USASA Field Station)
(U) [redacted]
(U) [redacted]
(U) [redacted]
(U) [redacted]
(U) [redacted]
(U) NSA Europe, Frankfurt, Germany
(U) NSA Europe, Stuttgart
(U) [redacted]
(U) Naval Security Group Activities (NSGAs) at Bremerhaven, Germany; [redacted] and [redacted]
(U) Rothwesten, Germany
(U) [redacted]

图 16 美国情报机构在德国设立的秘密情报站

[3] https://www.spiegel.de/international/world/german-intelligence-worked-closely-with-nsa-on-data-surveillance-a-912355.html

[4] https://www.theguardian.com/us-news/2020/feb/11/crypto-ag-cia-bnd-germany-intelligence-report

美国国家安全局（NSA）长期对德国总理、外交部长、驻外大使和总领事等政府高级官员的通信内容进行监听，监听内容广泛，其中不乏德国政府对国际形势和突发事件的看法，以及德国官员参与对美国际交流后的私下讨论，涉及政治、军事、经济、外交、政策、民族、安全、资源等重要领域。值得一提的是美国情报部门对欧盟国家的内部考虑，特别是对防范金融风险的解决方案有着浓厚兴趣（如图 17 所示）。



Germans, French Pursue New EU Treaty; Sweden May Be on Board Owing to Anger at UK (TS//SI-G//OC/REL TO USA, FVEY)

(TS//SI-G//OC/REL TO USA, FVEY) France and Germany were looking ahead in mid-December to a new EU treaty aimed at preventing future financial crises such as the one now plaguing the union, as an official at the Elysee Palace sought to inform German Chancellor Angela Merkel that President Nicolas Sarkozy preferred to start the process with a "friendly" meeting and joint reflection rather than a true working session. Regarding the drafting of a new treaty, German Chancellery EU Affairs Chief Nikolaus Meyer-Landrut advised on 13 December that his French interlocutor, Presidency Secretary-General Xavier Musca, agreed that EU Council President Herman van Rompuy should consult first with the most-important member states on the possible proper structure before a text was circulated for consideration. Landrut also indicated that Sweden is giving serious thought to signing on to the new treaty because of Stockholm's outrage at the UK's refusal to participate.

SCS

German leadership

G/J2/520014-11, 141624Z

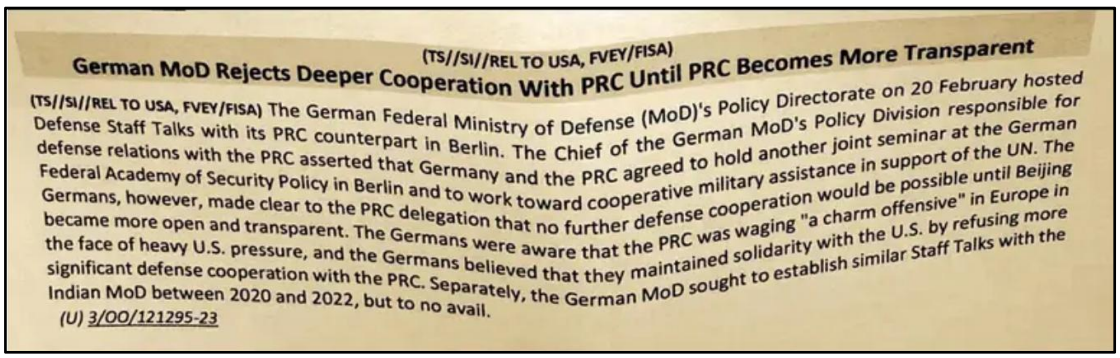
图 17 美国国家安全局（NSA）对德国政府领导人的监听记录

即便是在斯诺登事件后，美国也没有放松对德国的监听工作，只是采用了更加隐蔽的方式。2021 年 5 月，丹麦媒体[5]曝光了美国国家安全局（NSA）与丹麦国防情报局（FE）合作，对途经

[5] https://www.dr.dk/nyheder/indland/forsvarets-efterretningstjeneste-lod-usa-spionere-mod-angela-merkel-franske- norske

丹麦的互联网光缆实施监听，而监听对象包括德国、瑞典、挪威和法国的国家领导人、高级政客和高级官员。其中，时任德国总理安格拉·默克尔、时任德国外交部长弗兰克·瓦尔特·施泰因迈尔和时任德国反对党领袖佩尔·施泰因布吕克等都是美国国家安全局美丹合作监视项目的主要监听对象。而在当时主持该监听项目的恰恰是时任美国副总统，现任美国总统乔·拜登。

该监听项目被媒体曝光后再次引发德国、法国等欧洲国家不满，时任德国总理默克尔和法国总统马克龙都公开表示美国针对盟友的监听活动是“不可接受的”。但美国显然毫不在意这些所谓“盟友”们的感受。2023 年 4 月，美国针对德国国防部的监听活动再次被曝光[6]。



(TS//SI//REL TO USA, FVEY/FISA)

German MoD Rejects Deeper Cooperation With PRC Until PRC Becomes More Transparent

(TS//SI//REL TO USA, FVEY/FISA) The German Federal Ministry of Defense (MoD)'s Policy Directorate on 20 February hosted Defense Staff Talks with its PRC counterpart in Berlin. The Chief of the German MoD's Policy Division responsible for defense relations with the PRC asserted that Germany and the PRC agreed to hold another joint seminar at the German Federal Academy of Security Policy in Berlin and to work toward cooperative military assistance in support of the UN. The Germans, however, made clear to the PRC delegation that no further defense cooperation would be possible until Beijing became more open and transparent. The Germans were aware that the PRC was waging "a charm offensive" in Europe in the face of heavy U.S. pressure, and the Germans believed that they maintained solidarity with the U.S. by refusing more significant defense cooperation with the PRC. Separately, the German MoD sought to establish similar Staff Talks with the Indian MoD between 2020 and 2022, but to no avail.

(U) 3/OO/121295-23

图 18 美国国家安全局针对德国国防部的监听记录

美国国家安全局绝密级文件显示（如图 18 所示），此次监听活动涉及 2023 年 2 月 20 日德国国防部与来访的中国国防部代表团进行的军事外交会议，监听记录显示，美国重点关注的是德

6 https://www.tagesschau.de/investigativ/kontraste/pentagon-papiere-leaks-bundesverteidigungsministerium- 100.html

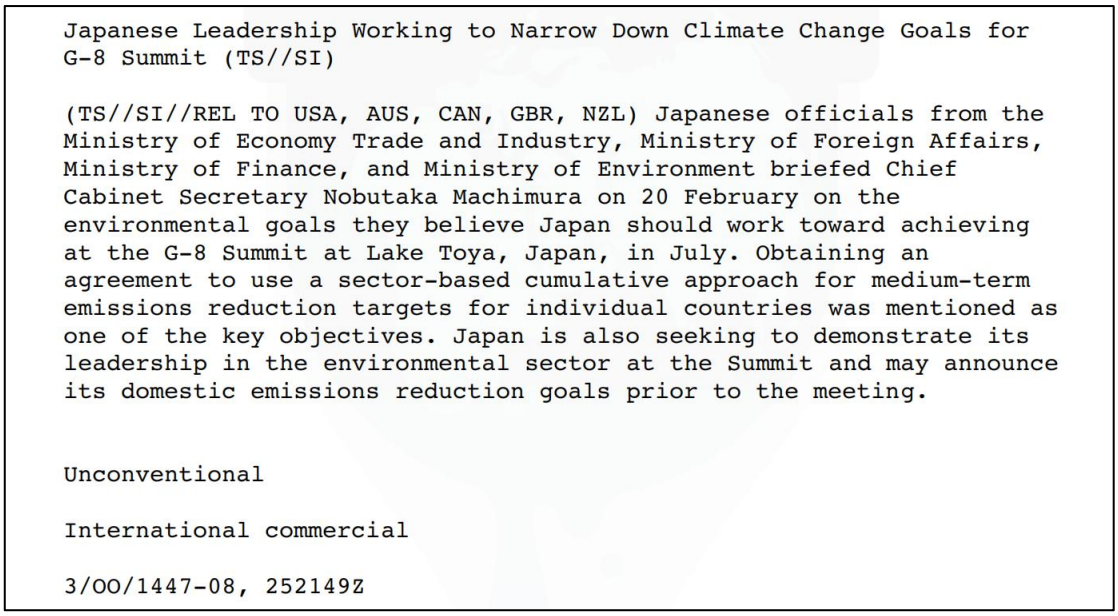
国在与中国进行军事领域合作问题上所持有的观点和立场。

2022 年，美国和欧洲建成新的跨大西洋数据传输框架，美国承诺将对欧洲的网络窃密活动进行更多监督，从而骗取欧洲同意将数据向美国流动。事实上，美国对欧洲盟友的网络窃密从未停止。

3、日本

美国国家安全局（NSA）对外窃听数据库中包含着涉及日本重要的政治和经济监听目标名单，该名单表明，美国国家安全局（NSA）对日本内阁、政府部门以及大型财团的间谍监听活动可以追溯到安倍政府。电话监听目标包括日本内阁办公场所的总机、时任内阁官房长官菅义伟的行政秘书、日本中央银行内部众多官员、三菱商事的天然气部门、三井物产的石油部门等等。其中一份题为《日本计划在八国集团峰会上公布的关于气候变化的机密提案》（如图 19 所示）更是明确标注了“REL TO USA，AUS，CAN，GBR，NZL”，表明该份情报已被美国政府高层正式授权与美国的“五眼联盟”盟友国家进行共享，为“五眼联盟”国家制订针对日本的专门计划创造条件，相关情报疑似从日本政府机构中隐蔽窃取，进一步显示了美国政府对日本政府监听活动的广泛性，具体内容涉及：农产品进口和贸易争端、日本在世界贸易组织多哈谈判中的立场、日本的气候变化政策、核能和能源政策

以及碳排放计划、日本与国际能源署（IEA）等国际机构间的通信，以及在安倍晋三官邸举行的首相简报会等重要情报，而实际情况远远不止于此。



Japanese Leadership Working to Narrow Down Climate Change Goals for G-8 Summit (TS//SI)

(TS//SI//REL TO USA, AUS, CAN, GBR, NZL) Japanese officials from the Ministry of Economy Trade and Industry, Ministry of Foreign Affairs, Ministry of Finance, and Ministry of Environment briefed Chief Cabinet Secretary Nobutaka Machimura on 20 February on the environmental goals they believe Japan should work toward achieving at the G-8 Summit at Lake Toya, Japan, in July. Obtaining an agreement to use a sector-based cumulative approach for medium-term emissions reduction targets for individual countries was mentioned as one of the key objectives. Japan is also seeking to demonstrate its leadership in the environmental sector at the Summit and may announce its domestic emissions reduction goals prior to the meeting.

Unconventional

International commercial

3/OO/1447-08, 252149Z

图 19 美国国家安全局（NSA）对日本领导人的监听记录

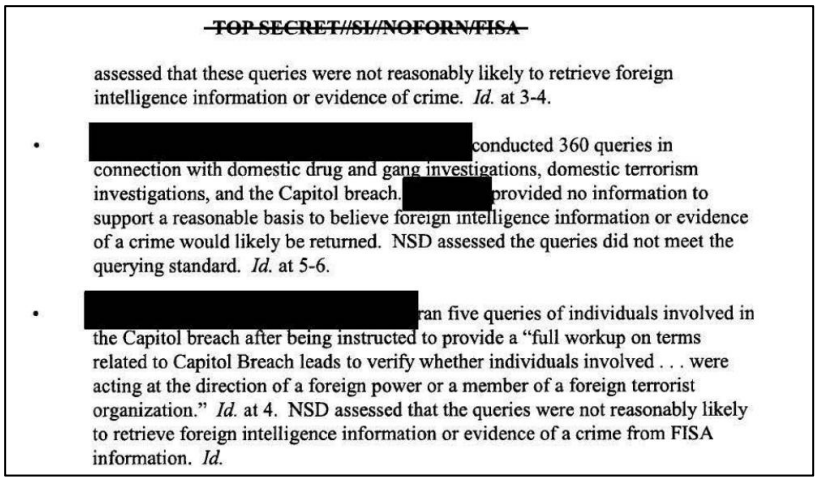
4、普通美国公民

我们在第二份调查报告中已经阐明，美国民间一直存在大量反对“702 条款”的正义声音。虽然“702 条款”表面上声称，美国国家安全局（NSA）等情报机构的情报收集活动只针对位于美国境外的外国人，但很明显，上面提到的美国国家安全局（NSA）监听计划的技术路线表明，这些监听计划的总体目标就是非法获取全球互联网用户的全量通信数据，这其中当然包括美国本土的美国公民，只是美国国家安全局（NSA）等美国情报机构在要求其情报分析人员在设置“情报查询筛选条件”（Selector）时，

“尽量”避免涉及美国本土的美国公民且不包含身处他国的“美国公民”，但这种几乎完全依靠“自律”的措施自然是形同虚设。2023 年 5 月 19 日，美国外国情报监视法院公开了一份文件[7]，揭示出美国情报机构曾经实施了数千次违反“702 条款”的行动（如图 20 所示），并特别指出，美联邦调查局（FBI）在搜集外国情报时，一再滥用通信和网络监听工具，对 2021 年 1 月 6 日美国国会山群体事件和 2020 年美国“黑命贵”自发维权抗争活动有关的美国公民进行监听，法院命令随后被媒体公开曝光并提出质疑[8]。实际上，在当年美国“占领华尔街”维权集会运动中，美国联邦调查局（FBI）、国家安全局（NSA）、中央情报局（CIA）等机构就对参加维权集会活动的所有现场及其联系人进行了全程无差别监听，并随后将这些活动手法用于中国台湾地区的“太阳花”骚乱活动和中国香港地区的“占中”非法集会活动中，可见对美国普通公民的监听也从未“缺席”。

[7] https://www.intelligence.gov/assets/documents/702%20Documents/declassified/21/2021_FISC_Certification_Opinion.pdf

[8] https://thehill.com/policy/national-security/4012650-fbi-misused-surveillance-tool-fisa-section-702/



~~TOP SECRET//SI//NOFORN/FISA~~

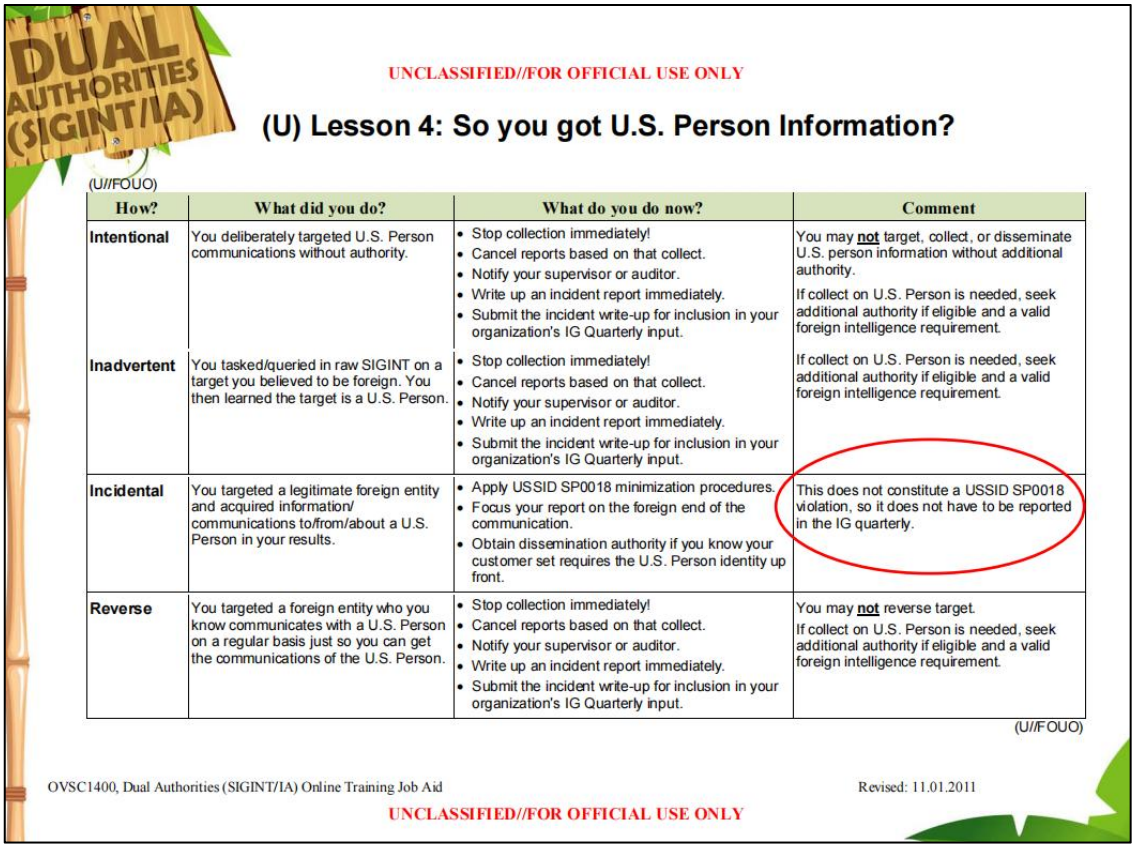
assessed that these queries were not reasonably likely to retrieve foreign intelligence information or evidence of crime. *Id.* at 3-4.

- [redacted] conducted 360 queries in connection with domestic drug and gang investigations, domestic terrorism investigations, and the Capitol breach. [redacted] provided no information to support a reasonable basis to believe foreign intelligence information or evidence of a crime would likely be returned. NSD assessed the queries did not meet the querying standard. *Id.* at 5-6.

- [redacted] ran five queries of individuals involved in the Capitol breach after being instructed to provide a "full workup on terms related to Capitol Breach leads to verify whether individuals involved . . . were acting at the direction of a foreign power or a member of a foreign terrorist organization." *Id.* at 4. NSD assessed that the queries were not reasonably likely to retrieve foreign intelligence information or evidence of a crime from FISA information. *Id.*

图 20. 美国外国情报监视法院公开文件中违反“702 条款”的案例

造成这种互联网监听“滥用”问题的主要原因，归根到底是由于美国情报机构在执行“702 条款”上采取了无限扩大化的宽松态度（如图 21 所示）。美国情报机构甚至在内部培训资料上明确指出，如果情报分析人员在工作过程中“偶然”查询到了美国公民的个人信息，并不违反规定，也不需要报告。



DUAL AUTHORITIES (SIGINT/IA)

UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) Lesson 4: So you got U.S. Person Information?

(U//FOUO)

How?	What did you do?	What do you do now?	Comment
Intentional	You deliberately targeted U.S. Person communications without authority.	• Stop collection immediately! • Cancel reports based on that collect. • Notify your supervisor or auditor. • Write up an incident report immediately. • Submit the incident write-up for inclusion in your organization's IG Quarterly input.	You may **not** target, collect, or disseminate U.S. person information without additional authority. If collect on U.S. Person is needed, seek additional authority if eligible and a valid foreign intelligence requirement.
Inadvertent	You tasked/queried in raw SIGINT on a target you believed to be foreign. You then learned the target is a U.S. Person.	• Stop collection immediately! • Cancel reports based on that collect. • Notify your supervisor or auditor. • Write up an incident report immediately. • Submit the incident write-up for inclusion in your organization's IG Quarterly input.	If collect on U.S. Person is needed, seek additional authority if eligible and a valid foreign intelligence requirement.
Incidental	You targeted a legitimate foreign entity and acquired information/ communications to/from/about a U.S. Person in your results.	• Apply USSID SP0018 minimization procedures. • Focus your report on the foreign end of the communication. • Obtain dissemination authority if you know your customer set requires the U.S. Person identity up front.	This does not constitute a USSID SP0018 violation, so it does not have to be reported in the IG quarterly.
Reverse	You targeted a foreign entity who you know communicates with a U.S. Person on a regular basis just so you can get the communications of the U.S. Person.	• Stop collection immediately! • Cancel reports based on that collect. • Notify your supervisor or auditor. • Write up an incident report immediately. • Submit the incident write-up for inclusion in your organization's IG Quarterly input.	You may **not** reverse target. If collect on U.S. Person is needed, seek additional authority if eligible and a valid foreign intelligence requirement.

(U//FOUO)

OVSC1400, Dual Authorities (SIGINT/IA) Online Training Job Aid

Revised: 11.01.2011

UNCLASSIFIED//FOR OFFICIAL USE ONLY

图 21. 美国情报机构关于“702 条款”合规性要求的培训材料

以上情况表明，美国的全球互联网监听计划及其所建立的监听站就如同网络空间中无处不在的“窥探者”，实时监听窃取全球互联网的用户数据，这种监听能力也成为美国构建“黑客帝国”和“窃密帝国”不可或缺的基石。而要维持这样庞大的监听计划，每年需要的经费预算相当惊人，随着互联网数据的爆炸式增长，美国全球网络监听计划对经费的需求也必然是“水涨船高”。这就是美国联邦政府及其情报机构合谋策划、推动“伏特台风”计划的主要动力。

而美国政客为了一己私利不惜欺骗国会的案例更是屡见不

鲜。在“伏特台风”计划的虚假叙事行动中扮演重要角色的美国联邦调查局（FBI）局长克里斯托弗·雷更是撒谎惯犯。2022 年 7 月，克里斯托弗·雷和美国司法部部长梅里克·嘉兰因掩盖现任美国总统拜登之子的罪证遭到参议员的质询[9]；2023 年 8 月，克里斯托弗·雷再次因为向国会提交虚假的备忘录文件[10]遭到多名众议院议员的质询；2024 年 7 月，克里斯托弗·雷又一次在美国国会关于美国前总统特朗普遭枪击案的听证会上作伪证并声称特朗普未被子弹击中[11]，同时还向国会隐瞒美国现总统拜登的真实健康状况。为此，特朗普强烈要求克里斯托弗·雷立即辞职。

四、事出反常必有妖

我们也注意到，在我们发布第二份关于“伏特台风”调查报告后，虽然美国官方机构与其主流媒体仍然保持沉默，但一些前任和现任美国政府机构官员以及部分美国网络安全公司通过社交媒体平台、美国的网络安全行业媒体和独立新闻媒体表达了对我方调查报告的观点与看法，其中不乏一些“步调一致”的负面声音，声称我方报告“歪曲”、“滥用”了美国相关公司的研究成果，这些美国公司也争先恐后地发声“撇清关系”。对此，我

[9] https://nypost.com/2022/08/31/fbi-agents-say-christopher-wray-has-got-to-go-report/

[10] https://nypost.com/2023/08/10/fbi-head-chris-wray-lied-about-targeting-catholics-he-owes-america-answers/

[11] https://www.nbcnews.com/politics/donald-trump/republicans-rip-fbi-directors-testimony-trump-might-not-hit-bullet-rcna163653

们有必要说明，在网络攻击事件的调查研究方面，引用和参考其他专业机构的研究成果是再正常不过的行业惯例。然而，仅仅因为得出不同的研究结论就被某些美国公司认为是“歪曲”和“滥用”，不仅让我们体会到美国网络霸权的影响力之大，而且更加让我们确信这些公司的表态必然是承受了巨大外部压力。

“威胁盟”公司的改口行为特别耐人寻味。该公司在接受媒体采访时声称，由于其在后续研究中发现了前期涉“伏特台风”报告中提供的感染指标存在错误才修改了原报告，这种“敷衍”的解释更加令人怀疑！且不说报告的修改时间存在很大疑点，原报告中被删掉的一整页内容中，不仅包含有 IP 地址列表，还包括命令控制服务器地址和勒索病毒的加密货币钱包地址等重要的关键性证据，难道这些证据在采集过程中全都出错的吗？“威胁盟”公司的科研态度，技术能力和技术素养何在？迫于美国政府机构的压力与其他“听话”美国网络安全机构的研究报告严格保持一致就是“威胁盟”的学术精神吗？另外，如果这种后续研究是详细而严谨的，那么在修改后的报告中为什么不进行解释说明，而且报告目录难道不应该一并进行修订吗？“威胁盟”这种异常举动，只能说明其对原报告的篡改过程是在强大外部压力下被动而匆忙完成的。当然，我们已经在最新报告中提供了更多的证据，这些证据充分表明美国情报机构对中国、俄罗斯、伊朗和

阿拉伯国家实施的网络间谍活动，以及针对美国国会和纳税人实施的虚假信息行动是铁一般的事实。

微软公司的回应也很值得关注，微软公司威胁情报战略总监德格里波（Sherrod DeGrippo）在 8 月 11 日 2024 年度黑帽大会（BlackHat）期间表示所谓的“伏特台风”组织仍在活跃，且没有停止的迹象，却仍然没有给出任何能够说明该组织具有所谓“中国政府支持背景”的确凿证据。实际上，2023 年以来，微软公司的举动就充满疑点，我们已经在前两篇报告中指出了微软公司显著加强了与美国军方和情报机构的合作。2024 年，这种合作更加深入。2024 年 5 月 7 日，据美国彭博社报道[12]，微软公司已经为美国情报机构部署了离线版本的人工智能大模型和助手程序，并被美国情报机构用于绝密级情报信息的辅助分析。更加令人担忧的是，微软公司表现出对用户“隐私信息”的超常关注。5 月 21 日，微软公司发布全新的人工智能解决方案“Copilot + PC”并推出“Recall”功能，使 Windows 操作系统可以记录用户所作的每一个操作，并提供给人工智能助手进行学习。尽管微软公司表示该功能仅限于本地运行，且数据被加密存储，但仍然无法打消用户对该功能被滥用而导致隐私泄露问题的疑虑。在巨大的争议声中，微软公司不得不推迟其随 Windows 更新推送的

[12] https://bloomberg.com/news/articles/2024-05-07/microsoft-create-top-secret-generative-ai-service-for-us- spies

该功能的计划。6 月 13 日，微软公司控股的 OpenAI 公司聘请美国国家安全局前局长中曾根担任董事会成员。微软公司的上述做法已经充分表明，作为“702 条款”相关监听项目的重要合作伙伴，微软公司受美国情报机构影响和操纵的程度日益加深。作为回报，美国政府机构则对微软公司滥用市场优势地位，利用 Windows 和 Office 更新捆绑推送软件产品变相实施垄断的行为“大开绿灯”。

在此，我们也不得不提到 7 月 19 日美国著名网络安全企业 CrowdStrike 公司产品的更新错误导致全球数百万台安装 Windows 操作系统的计算机“蓝屏”停止工作，并给多国公共交通、卫生健康等关键信息基础设施行业造成严重损失的网络安全事故。这样的事故是全球网络安全从业者都不希望看到的，特别是作为计算机病毒防治领域的从业者，这样的事故必将沉重打击用户对第三方杀毒软件产品的信心，进而影响全球网络安全行业生态。然而，对于造成如此严重后果的网络安全事故，作为美国最主要的网络安全主管部门，美国网络安全与基础设施安全局（CISA）却对微软公司和 CrowdStrike 公司异常“宽容”，不仅毫无作为，其局长简·伊斯特丽还在黑帽大会上将此次事故称为“伏特台风”组织攻击的“预演”，主动为微软公司和 CrowdStrike 公司解围和转移公众视线。这些违反常识且厚颜无耻的言论和行

为，当然有其深刻的原因背景。实际上，此次事故恰恰体现了美国在IT供应链上的巨大优势，微软公司和CrowdStrike公司作为美国情报机构的重要合作伙伴，当然会得到美国政府机构的“庇护”。微软公司和CrowdStrike公司不仅不会遭到处罚，反而会在美国政府机构的“保驾护航”下，打着“中国网络威胁论”的旗号，在全球市场继续“攻城略地”，并为“702条款”源源不断的输送情报。

与此同时，我们也注意到，很多来自美洲、欧洲、亚洲、非洲的知名媒体、国际人士和行业专家也纷纷就“伏特台风”的真相发出了正义的声音。特别是来自澳大利亚的专家发表了名为《网络间谍活动的地缘政治》[13]专题评论文章，明确指出美国政府和微软公司的报告缺乏确凿证据，并再次揭示了美国情报机构为进一步扩大无证监视权力，通过编造“伏特台风”网络攻击威胁获取公众支持和向政策制定者施压的丑陋行径。对这些国际正义人士的仗义执言我们深表敬意。

五、结语

多年来，美国联邦政府机构出于自身一己私利，不断将网络攻击溯源问题政治化，一些像微软和CrowdStrike这样的公司则为了迎合美国政客、政府机构和情报机构，出于提高自身商业利

[13] https://johnmenadue.com/the-geopolitics-of-cyber-espionage/

益考虑，在缺乏足够证据和严谨技术分析的情况下，热衷于用各种各样稀奇古怪且带有明显地缘政治色彩的名字对黑客组织进行命名，如“台风”“熊猫”和“龙”等，而不是“盎撒”“飓风”和“考拉”，以显示自己所谓的“高超”技术和文化底蕴，结果却忽视了最基本的产品质量问题，带坏了整个行业风气。我们在前期报告中多次重申，中国一向反对政治操弄网络安全事件的技术调查，反对将网络攻击溯源归因问题政治化。而美国联邦政府机构则不断在幕后教唆纵容，在通过编造子虚乌有的网络攻击威胁骗取了大量国会预算后，野心越来越大，终有一天将会“搬起石头砸自己的脚”。克里斯托弗·雷等美国无良政客为谋取不正当利益，频繁登场操弄“伏特台风”虚假叙事欺骗美国国会和民众，也必将遭到美国人民对其的正义审判。

最后，在地缘政治冲突不断加剧的今天，国际间正常的交流恰恰是网络安全行业最需要的，我们也再次呼吁，网络安全需要广泛的国际协作，广大网络安全企业和研究机构也应该专注于对网络安全威胁对抗技术的研究以及如何为用户提供更高质量的产品和服务，使互联网在促进人类社会共同发展进步中行稳致远。

国家计算机病毒应急处理中心

计算机病毒防治技术国家工程实验室

2024 年 10 月 14 日