国家计算机病毒应急处理中心
NATIONAL COMPUTER VIRUS EMERGENCY RESPONSE CENTER

Volt Typhoon III

— Unraveling Cyberespionage and Disinformation Operations Conducted by U.S. Government Agencies

Abstract: After the release of the first two investigation reports on Volt Typhoon, the U.S. federal government, mainstream media, and Microsoft have remained silent collectively. However, former and current U.S. intelligence agencies and security network officials represented by Robert Joyce, as well as some U.S. network security companies and media have spoken out and strained every nerve to quibble, while keeping silent on the evidence we published in the previous two reports, once again fully exposing their guilty conscience. Based on the previous two reports, this report further discloses that the U.S. federal government, intelligence agencies and Five Eyes countries jointly conducted cyber espionage eavesdropping activities against other countries such as China and Germany, and Internet users around the world. There's ironclad evidence that they blame other countries through the misleading traceability

attribution analysis of the stealth toolkit to carry out False Flag operations and cover up their own malicious cyberattacks. And the fact that the U.S. adopted supply chain attacks, implanted backdoors in Internet products and “pre-positioned” has completely debunked the Volt Typhoon – a political farce written, directed and acted by the U.S. federal government.

I. Introduction

The two reports entitled *Volt Typhoon: A Conspiratorial Swindling Campaign targeting U.S. Congress and Taxpayers conducted by U.S. Intelligence Community*[1] and *Volt Typhoon II: A secret Disinformation Campaign targeting U.S. Congress and Taxpayers conducted by U.S. Government agencies*[2] were jointly released by China’s National Computer Virus Emergency Response Center (CVERC), National Engineering

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

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

Laboratory for Computer Virus Prevention Technology and 360 Digital Security Group on April 15 and July 8, 2024. The reports comprehensively exposed the House of Cards farce in which the U.S. government agencies continue to control the so-called “warrantless surveillance rights” to indiscriminately monitor global telecommunications and Internet users, obtain greater political and economic interests for the relevant interest groups behind it, fabricating the so-called danger of Chinese cyberattacks, and conspiring to defraud U.S. Congressmen and taxpayers. After the release of the reports, the lie makers, the U.S. Agency for Global Media, and the mainstream media in the U.S. and the West under their control remained silent as always, which nevertheless attracted widespread attention in the international community. More than 50 cybersecurity experts from the U.S., Europe, Asia and other countries and regions contacted

CVERC via various means. They believed that the U.S. and Microsoft lacked effective evidence to associate Volt Typhoon with China, and expressed concern about the U.S. false narrative of Volt Typhoon. Meanwhile, the rising popularity of relevant topics online has made the international community more clearly understand the real purpose of the U.S. and its cyber hegemony, and the real harm of the U.S. indiscriminate monitoring of the world with Internet. Therefore, it is necessary for us to disclose more objective evidence of the U.S. government agencies' involvement in fabricating the false narrative of Volt Typhoon, organizing and implementing False Flag operations, and launching cyberattacks against China, and continue to reveal the U.S. tricks of a robber acting like a cop, or an ostrich burying its head in the sand.

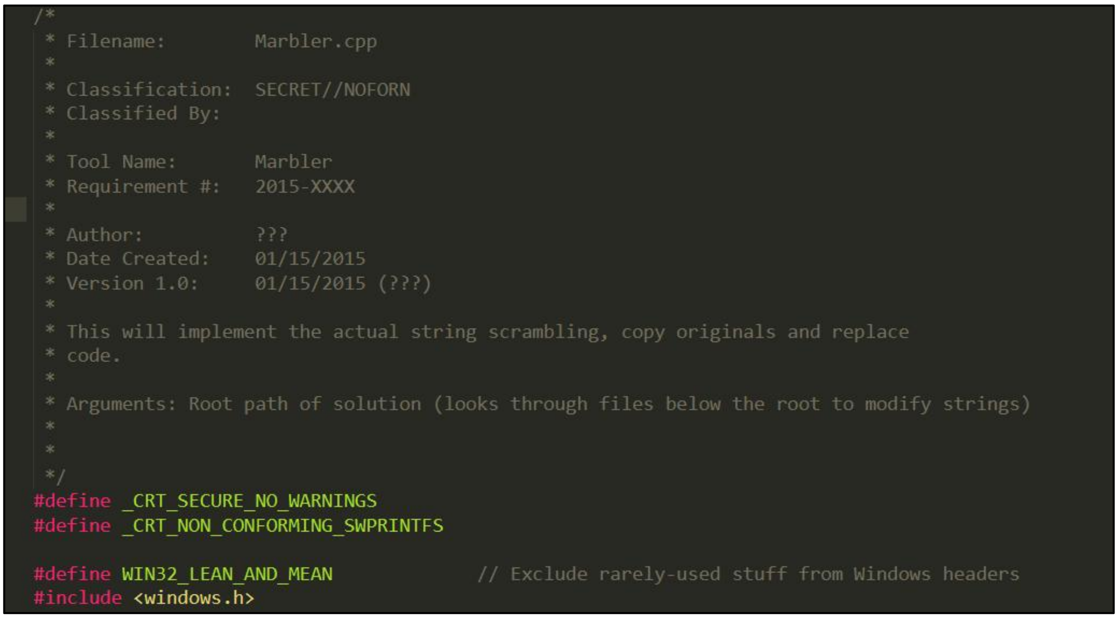
II. "Chameleons" in Cyberspace

As is known to all, the U.S. is the world’s largest arms supplier. The huge military-industrial system and powerful military-industrial complex have become significant cornerstones of its political, economic, and military policies. The resulting cyber arsenal is not only large in scale and diverse in form, but also complex in function and rich in products. Previously, the CVERC has publicly disclosed a number of cyber weapons developed by the U.S. National Security Agency (NSA) and Central Intelligence Agency (CIA). The investigation report on the NSA’s network attacks on China’s Northwest Polytechnical University made a detailed analysis of the function of the various weapons used by the U.S. intelligent agencies in external cyberattacks, as well as the highly stealthy attack techniques and tactics. However, those are apparently only the tip of the iceberg of the U.S. cyber arsenal.

For a long time, the U.S. has actively

pursued the strategy of “forward defense” in cyberspace and carried out “hunt forward” tactical operation, i.e., deploying cyber warfare forces around the adversary countries to carry out close reconnaissance and cyber infiltration of cyber targets. To meet the tactical requirements, the U.S. intelligence agencies developed a special stealth toolkit codenamed “Marble” to cover up their own malicious cyberattacks, blame other countries, and mislead traceability attribution analysis. The toolkit is a tool framework that can be integrated with other cyber weapon development projects to assist cyber weapon developers in obfuscating various identifiable features in program code, effectively “erasing” the “fingerprints” of cyber weapon developers, similar to changing the “rifling” of “firearm” weapons, shifting the direction of weapons, and making it impossible for investigators to trace the true source of weapons from a technological perspective. What’s more, the framework has a more “shameless” function to insert strings in other languages, such as Chinese, Russian, Korean, Persian, and Arabic, which is obviously intended to mislead investigators and frame China, Russia, North Korea, Iran, and Arab countries.

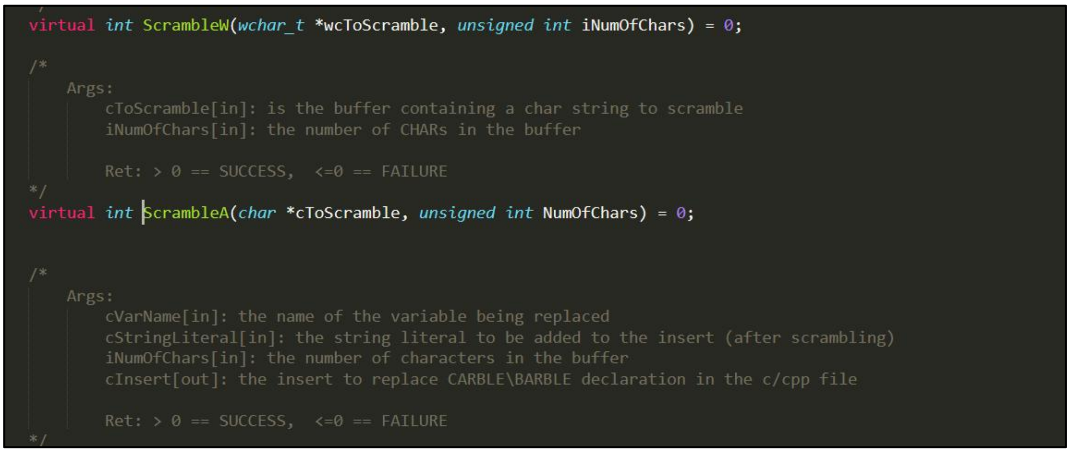
According to the Marble tool framework source code and its annotations (as shown in Figure 1), it was identified as a classified (and non-disclosable) weapon development program that began no later than 2015. Obviously, it was a secret weapon tailored for itself by the U.S. intelligence agencies, and it was strictly forbidden to even disclose to the so-called “allied” countries.



```
/*
 * 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>
```

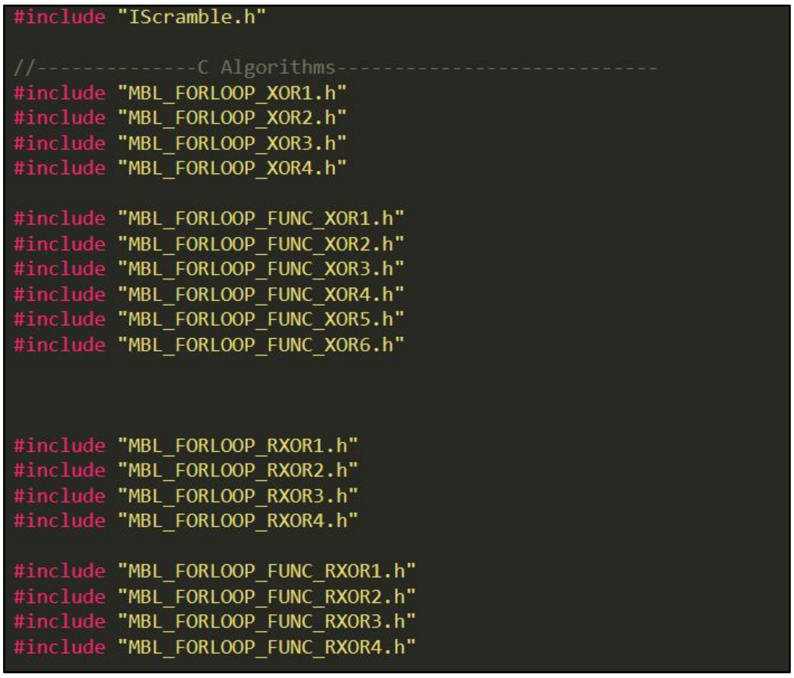
Figure 1 Source code of Marble

The Marble’s tool framework can use over 100 obfuscation algorithms to replace readable variable names, strings, and so on, in source code files with unreadable (unrecognizable) content, and can insert specific interfering strings (as shown in Figures 2, 3, 4 and 5).



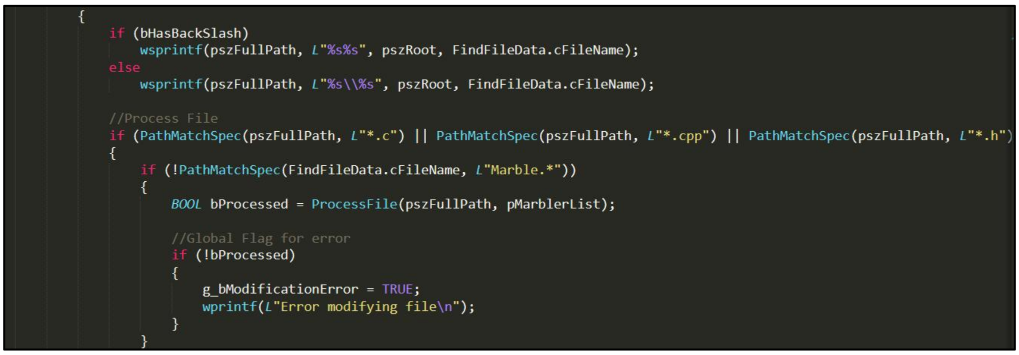
```
virtual int ScrambleW(wchar_t *wcToScramble, unsigned int iNumOfChars) = 0;

/*
    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
*/
```

Figure 2 Obfuscation functions



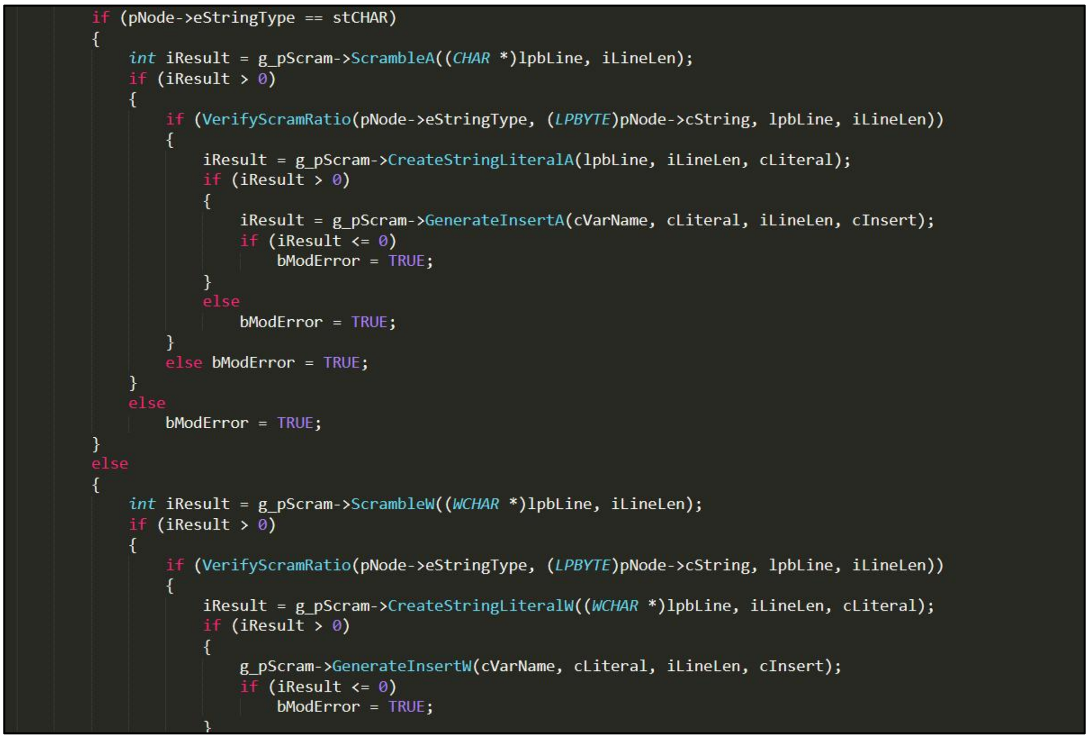
```
#include "IScramble.h"

//-------------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"
```

Figure 3 Obfuscation algorithms



```
{
    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");
            }
        }
```

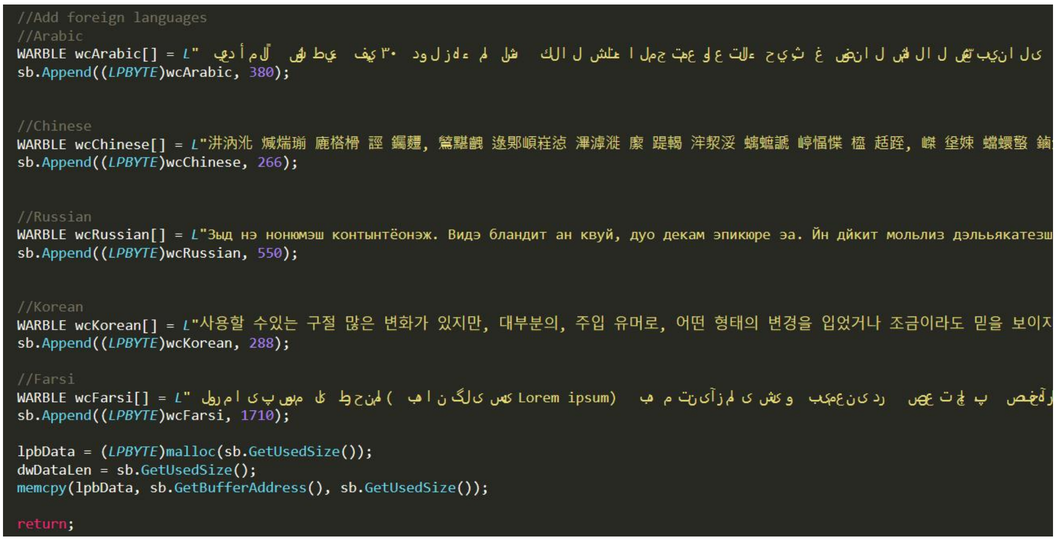
Figure 4 File handling functions



```
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;
            }
```

Figure 5 File handling functions (continued)

We can even find out which foreign language strings can be inserted from the source code of the test example of Marble, which includes only Arabic, Chinese, Russian, Korean, and Persian (as shown in Figure 6).



```
//Add foreign languages
//Arabic
WARBLE wcArabic[] = L" أديب لمآ  عيط ىلق  ٣٠ يف  دو لزج ءة م  لش  كلال ل علش ا لمج عمت ول ع ءلات ح يثو غ  ضنا ل ىش لا ل تعبين ال ى
sb.Append((LPBYTE)wcArabic, 380);


//Chinese
WARBLE wcChinese[] = L"洴汭兆 熸煓瑜 鹿榙榗 誙 鑷趩, 鷥鷃齯 逯郢頙崹浤 潬瀌洴 縻 踶輵 浲絜涭 螭蠦謕 崿愊愥 榼 趏踁, 嵥 坌婖 蟷蠉螯 鍎
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 ا یپ سوم ک طوح نل ( با ن گلی سک Lorem ipsum)  ب م تن ای زمل ی شک و  بفم ع ن ی در  صع ت چ پ  صخهآر
sb.Append((LPBYTE)wcFarsi, 1710);

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

return;
```

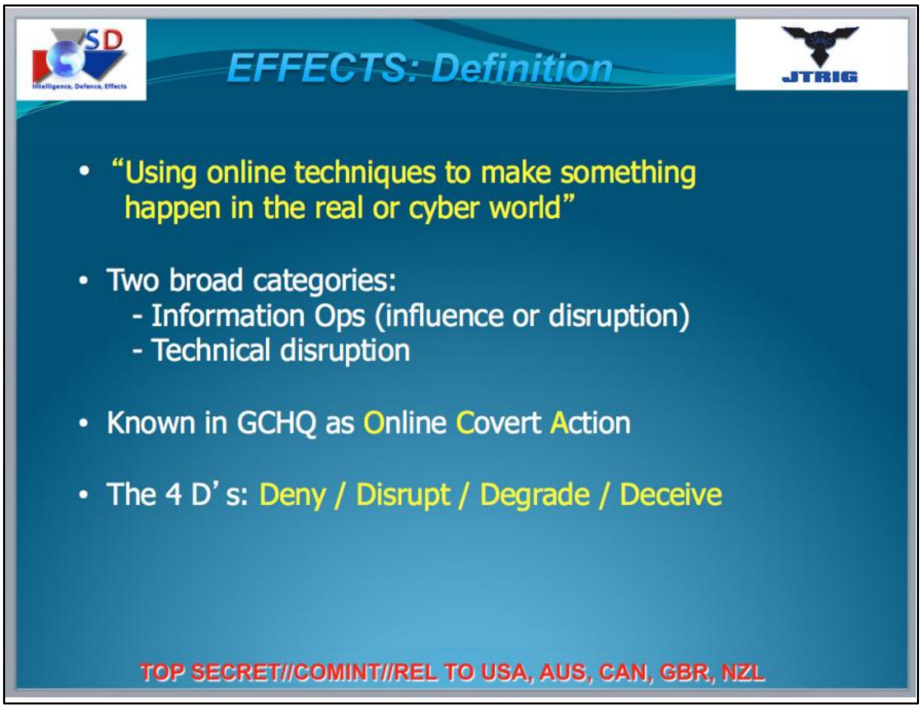
Figure 6 Inserting foreign languages into a file

The Marble toolkit framework fully exposes the indiscriminate and bottomless cyberespionage activities and False Flag operations carried out by the U.S. intelligence agencies around the world to mislead investigators and researchers and realize the conspiracy of smearing adversary countries.

False Flag operations are not limited to code signatures. By cleverly mimicking the attack techniques and tactics of cybercrime gangs, the U.S. intelligence agencies can also create all kinds of perfect “pocket” organizations, which has already been explained in our second report.

Therefore, the U.S. cyber warfare forces and hackers in intelligence agencies act like chameleons in cyberspace to change identities and images at will, to “represent” other countries to carry out cyberattacks and theft around the world, and smear non-allied countries.

According to reliable sources, False Flag operations are actually a major component of Influence Operations by the U.S. intelligence agencies. Secret documents from the U.S. and the Five Eyes countries show that Influence Operations mainly include two aspects: Information Operations and Technical Disruption Operations. The NSA has developed a playbook for Technical Disruption Operations, and False Flag operations are an important component. Internal documents from the U.S. and the Five Eyes countries also make it clear that the 4D principles, namely, deny, disrupt, degrade, and deceive, must be observed in the implementation of Influence Operations. The 4Ds cover all the core elements of Volt Typhoon (as shown in Figures 7 and 8).



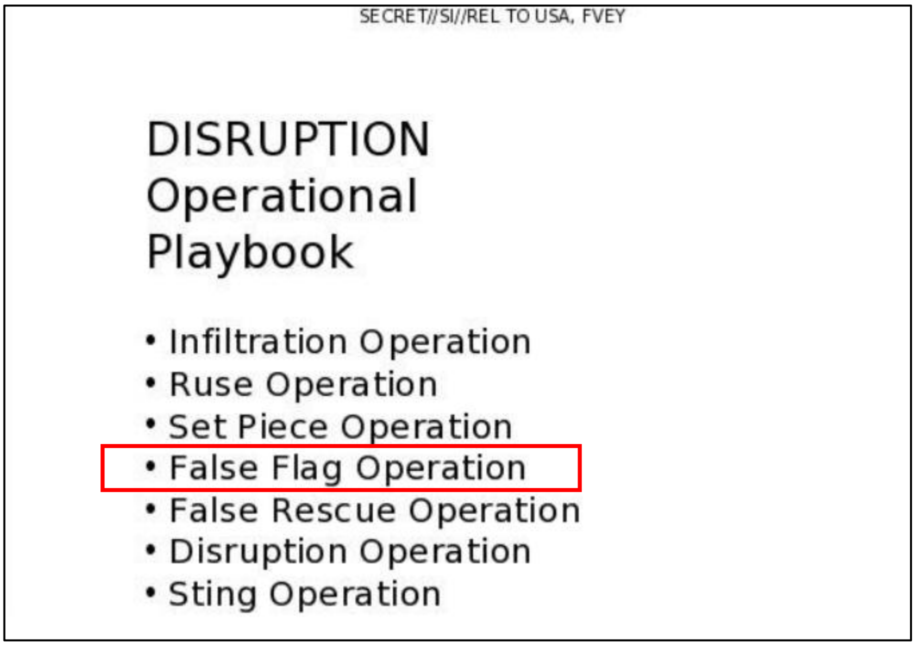
EFFECTS: Definition

- "Using online techniques to make something happen in the real or cyber world"
- Two broad categories:
  - Information Ops (influence or disruption)
  - Technical disruption
- Known in GCHQ as Online Covert Action
- The 4 D's: Deny / Disrupt / Degrade / Deceive

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

SD
Intelligence, Defence, Effects
JTRIG

Figure 7 The definition of Influence Operations by the U.S. and the Five Eyes countries



SECRET//SI//REL TO USA, FVEY

DISRUPTION
Operational
Playbook

- Infiltration Operation
- Ruse Operation
- Set Piece Operation
- False Flag Operation
- False Rescue Operation
- Disruption Operation
- Sting Operation

Figure 8 Disruption Operational Playbook by the U.S. and the Five Eyes countries

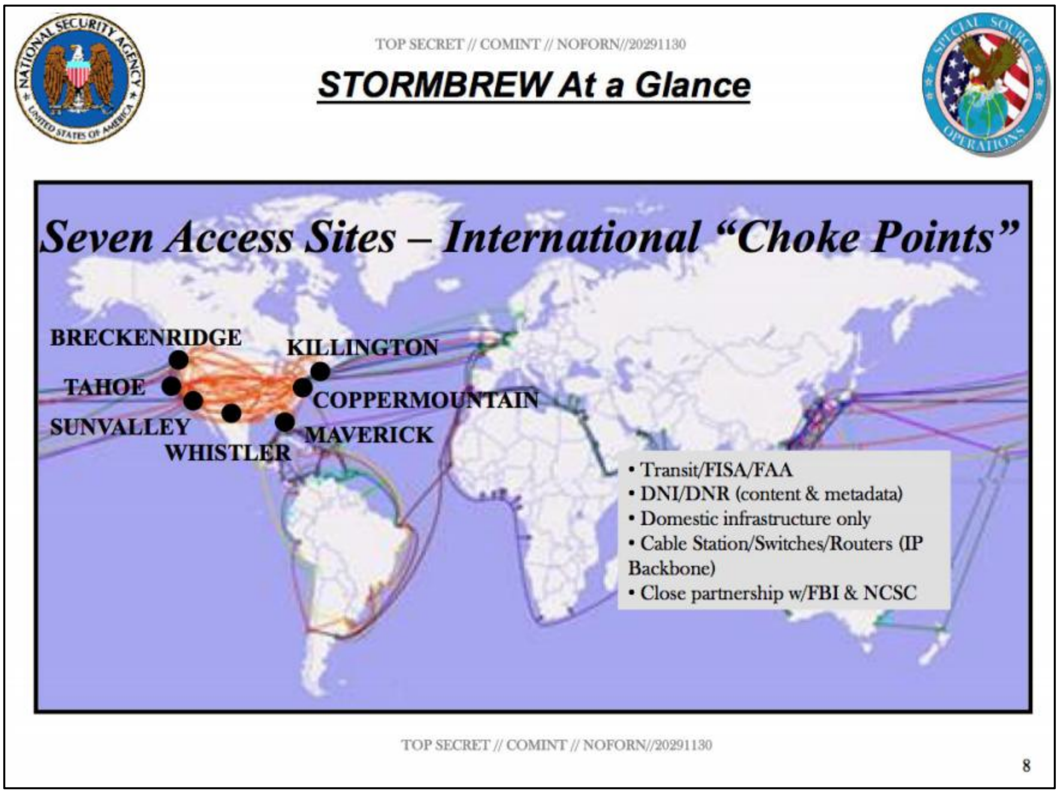
From the above evidence, it can be inferred that Volt Typhoon is a typical, well-designed disinformation operation (the so-called False Flag operation) in the interest of the U.S. capital group. Its techniques and tactics are fully consistent with those used by the U.S. and the Five Eyes countries' intelligence agencies in Influence Operations. It is of course very difficult to see through this hoax elaborated by the U.S. intelligence agencies. Due to the large amount of interfering information, it is far from enough to rely on technological analysis alone. It is necessary to comprehensively analyze the information and relevant materials of multiple parties to discover the negligence and mistakes inadvertently exposed by the U.S. intelligence agencies, and to correctly understand and interpret the sinister plans concocted by intelligence agencies such as the NSA and CIA. That's what we did in the last two reports (*Volt Typhoon: A Conspiratorial Swindling Campaign targets with U.S. Congress and Taxpayers conducted by U.S. Intelligence Community* and *Volt Typhoon II: A secret Disinformation Campaign targeting U.S. Congress and Taxpayers conducted by U.S. Government agencies*).

III. "Snoopers" in Cyberspace

In the second report, we exposed the political scandal of the U.S. federal agencies, especially intelligence agencies, which fabricated the so-called "external cyber threats" and launched disinformation operations in order to maintain their massive indiscriminate surveillance programs to maintain their unwarranted powers under Section 702 of the Foreign Intelligence Surveillance Act (FISA). In this report, we will further disclose the details of the above-mentioned surveillance program.

(I) Choking the "Throat" of Internet

According to the NSA's internal top-secret data (as shown in Figure 9), the U.S. relies on its innate technological advantages and geological advantages in the construction of the Internet to firmly control the world's most important Internet choke points such as the Atlantic submarine fiber optic cable and the Pacific submarine fiber optic cable. It has successively established seven national-level full-traffic monitoring stations. The NSA works closely with the Federal Bureau of Investigation (FBI) and the British National Cyber Security Center (NCSC) to carry out protocol analysis and data theft of the full amount of data transmitted in fiber optic cables, so as to achieve indiscriminate monitoring of Internet users around the world.



TOP SECRET // COMINT // NOFORN//20291130

STORMBREW At a Glance

Seven Access Sites – International "Choke Points"

- Transit/FISA/FAA
- DNI/DNR (content & metadata)
- Domestic infrastructure only
- Cable Station/Switches/Routers (IP Backbone)
- Close partnership w/FBI & NCSC

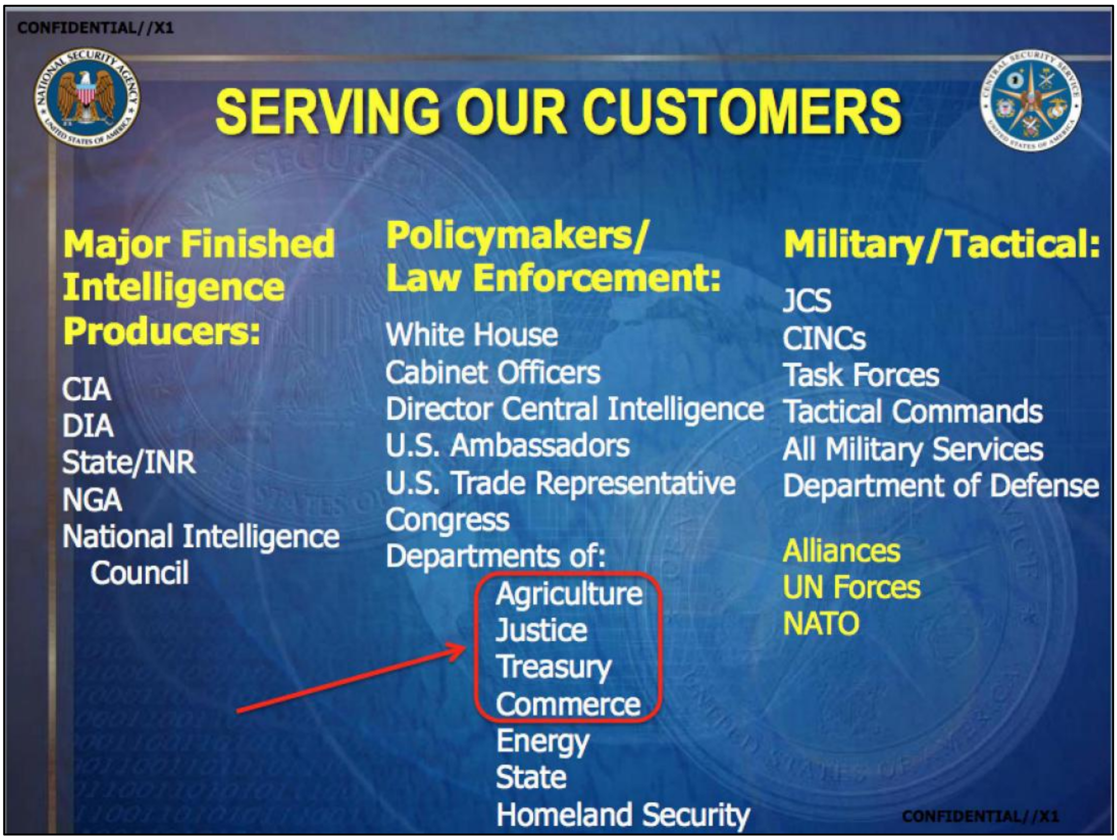
TOP SECRET // COMINT // NOFORN//20291130

8

Figure 9 Submarine fiber optic cable monitoring stations established and operated by the NSA

There are many beneficiaries of the Internet data surveillance and signal intelligence. In addition to U.S. intelligence agencies and military agencies, there are a large number of federal government departments, including the White

House, cabinet officials, U.S. embassies abroad, Office of the U.S. Trade Representative, the U.S. Congress, as well as the U.S. Department of State, Department of Agriculture, Department of Justice, Department of Treasury, Department of Energy, Department of Commerce, Department of Homeland Security, etc. That is what we pointed out in the second report: The participants in Volt Typhoon were not limited to U.S. intelligence agencies, but were intended to serve the common interests of the so-called U.S. capital. Many U.S. government agencies have helped intensify the strength of billows and waves (as shown in Figure 10).



CONFIDENTIAL//X1

SERVING OUR CUSTOMERS

Major Finished Intelligence Producers:

CIA
DIA
State/INR
NGA
National Intelligence Council

Policymakers/ Law Enforcement:

White House
Cabinet Officers
Director Central Intelligence
U.S. Ambassadors
U.S. Trade Representative
Congress
Departments of:
Agriculture
Justice
Treasury
Commerce
Energy
State
Homeland Security

Military/Tactical:

JCS
CINCs
Task Forces
Tactical Commands
All Military Services
Department of Defense

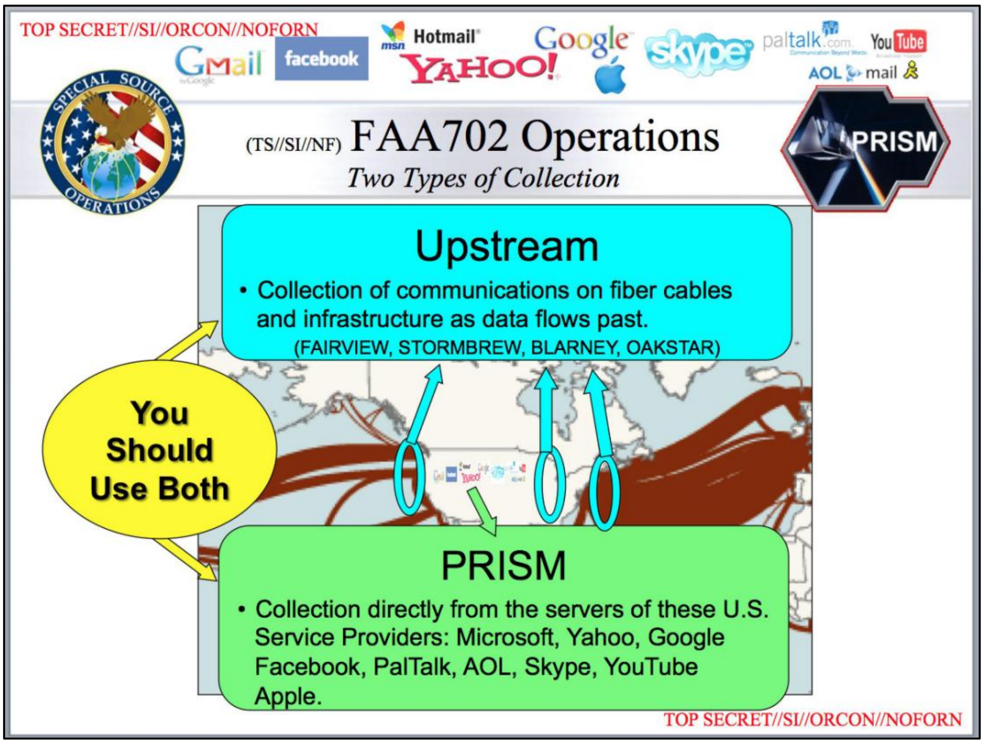
Alliances
UN Forces
NATO

CONFIDENTIAL//X1

Figure 10 Customer list of the NSA intelligence

(II) Controlling the "Reservoir" of Internet Data

The output of intelligence surveillance is inevitably all kinds of readable information and data. Therefore, it is another important task of the NSA to convert and translate the transmission traffic in the submarine fiber optic cable into readable and retrievable intelligence information in real time. With the growing proportion of encrypted network traffic, this work has also encountered tremendous challenges. To cope with the situation, the NSA has implemented two key engineering projects. **The first is the UpStream project,** whose main function is to retain all the original communication data of the submarine fiber optic cables intercepted by the above-mentioned monitoring stations in a massive-scale data "reservoir." The enormous original data in the "reservoir" is the "upstream" of the follow-up intelligence processing workflow. It is worth noting that during the United Nations General Assembly recently, the U.S. and some of its allies issued a joint statement, declaring to maintain the safety and reliability of submarine cables. **The second is the Prism project,** whose major function is, on the one hand, to classify the original data in the UpStream project according to the Internet application, and to analyze the content; on the other hand, to effectively address the prominent problems of encrypted data cracking and incomplete coverage of network communication traffic paths in the UpStream project. The U.S. government mandated that the Prism project directly obtain user data from the servers of major U.S. Internet companies, including Microsoft, Yahoo, Google, Facebook (which has been renamed Meta), Apple, etc. Both projects were built under the authority of Section 702, which has become not only the official basis for U.S. intelligence agencies to legally, openly, and continuously steal global Internet link data on behalf of the U.S. federal government, but also the solid and undeniable evidence of data theft (as shown in Figure 11).



TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) FAA702 Operations

Two Types of Collection

Upstream

- Collection of communications on fiber cables and infrastructure as data flows past.

(FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR)

You Should Use Both

PRISM

- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google Facebook, PalTalk, AOL, Skype, YouTube Apple.

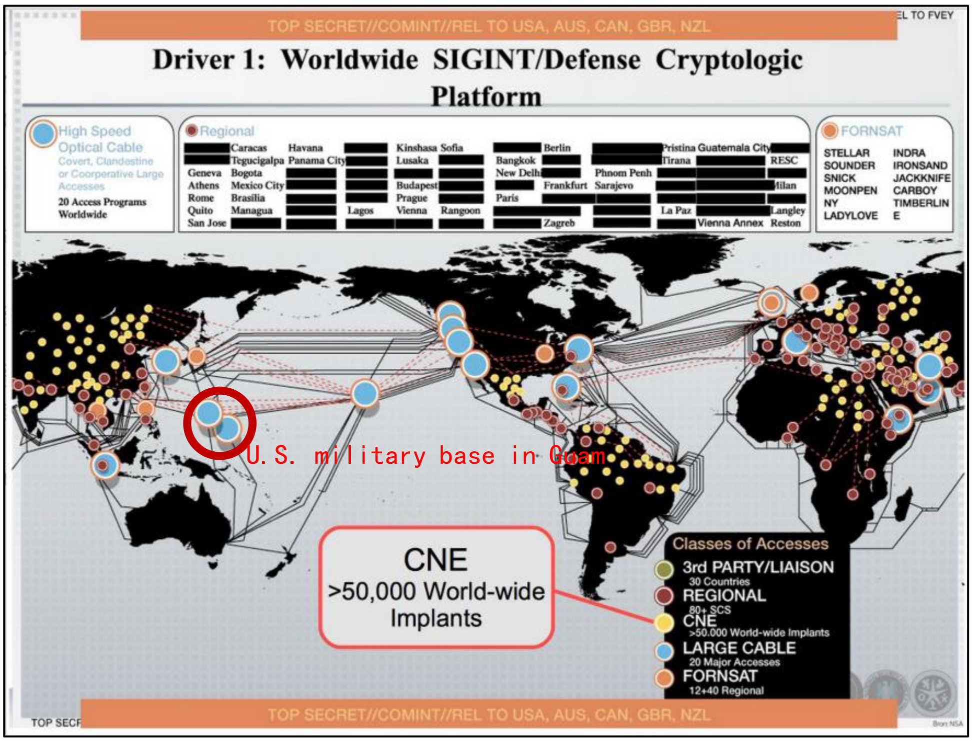
TOP SECRET//SI//ORCON//NOFORN

Figure 11 Two key projects for global Internet surveillance conducted by the NSA

(III) Diving into the “Source” of Internet Data

Although the NSA has deployed a large number of surveillance systems on the Internet, if the targets of these systems and their network communication contents stay only in specific areas covered by submarine fiber optic cables, the data stolen by these monitoring systems would be far from satisfying the NSA’s appetite for intelligence. To solve the problem, the NSA has conducted Computer Network Exploitation (CNE) for specific targets located in the blind spots of the monitoring system, and the NSA’s notorious Office of Tailored Access Operation (TAO) is the one that has done this dirty work. According to top-secret NSA documents, the TAO has launched indiscriminate CNEs around the world and implanted more than 50,000 Implants (a spyware), with targets in Asia, Eastern Europe, Africa, the Middle East and South America. Almost all major cities in China are within CNE, and a large number of Internet assets have been compromised, including those in the regions where the Northwestern Polytechnical University and Wuhan Earthquake Monitoring Center are located. Many of the command-and-control centers for these spyware programs are located at military bases outside the U.S. mainland, including those in Japan, Korea, Guam and Hawaii. **Guam,** which is familiar to readers who have followed our first two reports, can be called the original source of Volt Typhoon fabricated by the U.S. government, and it will forever be recorded in the cybersecurity development history because of the false narrative of Volt Typhoon. As a matter of fact, the U.S. military base in Guam has not been a victim of the Volt Typhoon cyberattacks at all, but the initiator of a large number of cyberattacks against China and many Southeast Asian countries and the backhaul center of stolen data (as shown in Figures 12 and 13).

For some high-value targets in other countries with a high level of protection, which are difficult to penetrate, the TAO would launch supply chain attacks. To be specific, relying on the advantages in advanced network security technology and products, and with the cooperation of large U.S. Internet companies or equipment suppliers, the Tao would intercept and disassemble the U.S. network products purchased by the targets, implant backdoors and repackage them for shipment to the targets. This method is often applied in the attack of telecommunications and network operators in other countries, which can realize the intrusion control of the target telecom operator’s call detail record billing and other systems, and realize the monitoring of the target’s mobile phone communication content. In the case of the TAO cyberattack on Northwestern Polytechnical University, relevant telecommunications and network operators in China were subject to such attacks. The target’s call content, Internet records and real-life activity tracks were all stolen by the TAO (as shown in Figure 14).



EL TO FVEY

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Driver 1: Worldwide SIGINT/Defense Cryptologic Platform

High Speed Optical Cable
Covert, Clandestine or Coorperative Large Accesses
20 Access Programs Worldwide

Regional
[redacted] Caracas Havana [redacted] Kinshasa Sofia [redacted] Berlin [redacted] Pristina Guatemala City [redacted]
[redacted] Tegucigalpa Panama City [redacted] Lusaka [redacted] Bangkok [redacted] [redacted] Tirana [redacted] RESC
Geneva Bogota [redacted] [redacted] [redacted] [redacted] New Delh [redacted] Phnom Penh [redacted] [redacted] [redacted]
Athens Mexico City [redacted] [redacted] Budapest [redacted] [redacted] Frankfurt Sarajevo [redacted] [redacted] ilan
Rome Brasilia [redacted] [redacted] Prague [redacted] Paris [redacted] [redacted] [redacted] [redacted] [redacted]
Quito Managua [redacted] Lagos Vienna Rangoon [redacted] [redacted] La Paz [redacted] Langley
San Jose [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] Zagreb [redacted] [redacted] Vienna Annex Reston

FORNSAT
STELLAR INDRA
SOUNDER IRONSAND
SNICK JACKKNIFE
MOONPEN CARBOY
NY TIMBERLIN
LADYLOVE E

CNE
>50,000 World-wide Implants

Classes of Accesses
● 3rd PARTY/LIAISON
30 Countries
● REGIONAL
80+ SCS
● CNE
>50.000 World-wide Implants
● LARGE CABLE
20 Major Accesses
● FORNSAT
12+40 Regional

TOP SECR

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Bron: NSA

Figure 12 Sketch map of the TAO’s global cyber intrusion operations

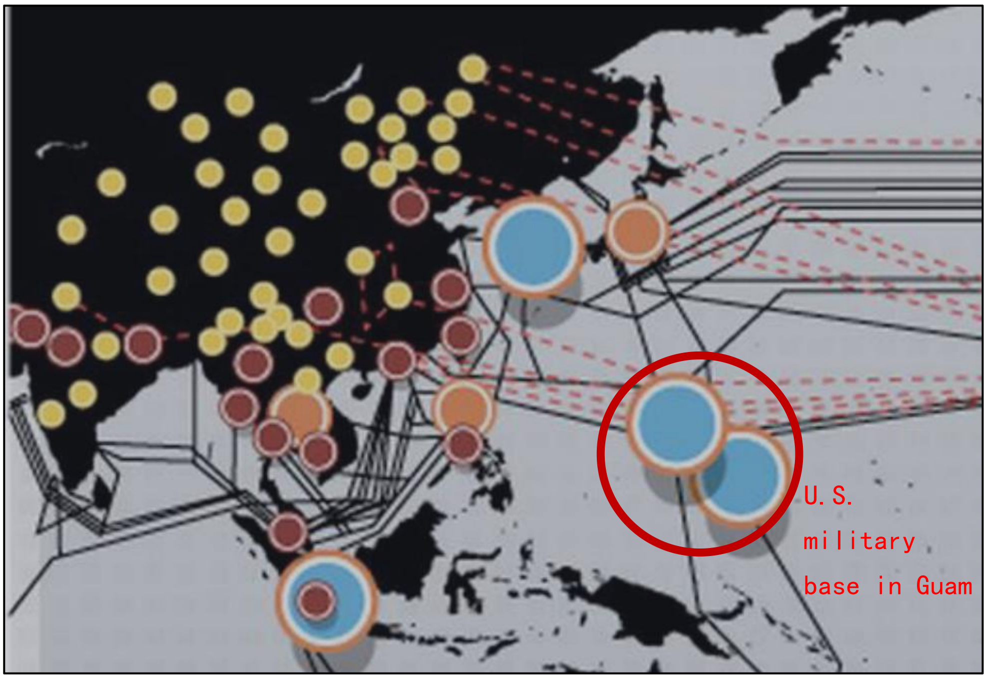
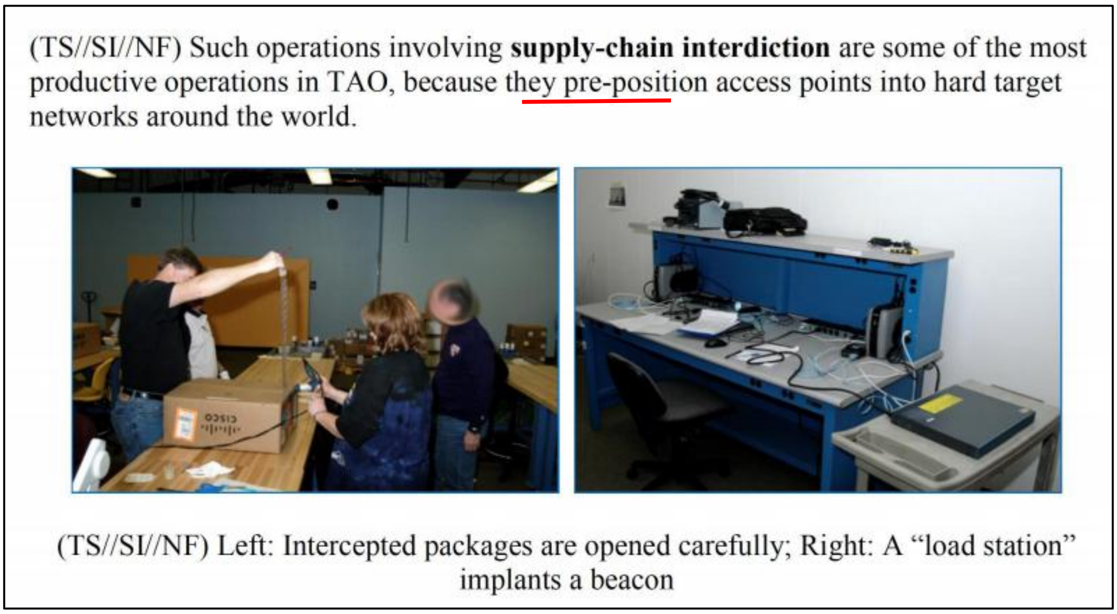


Figure 13 Sketch map of the TAO’s cyber intrusion in China



(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

Figure 14 The TAO technicians disassemble the Cisco network equipment purchased by the monitoring target and implant a backdoor

Ironically, the NSA used the tactical term pre-position to describe this kind of supply chain attack, which specifically refers to the preset backdoor virus in the Internet products used by the monitoring target, laying the groundwork for the NSA's subsequent attack, control and theft activities. We found that the term pre-position was also used by the U.S. federal agencies to describe the tactics used by Volt Typhoon to conduct cyberattacks on critical infrastructure based in places like Guam. So, who on earth has pre-positioned in the world's critical infrastructure? The facts are already very clear.

(IV) "Making Exorbitant Demand" for Internet Intelligence

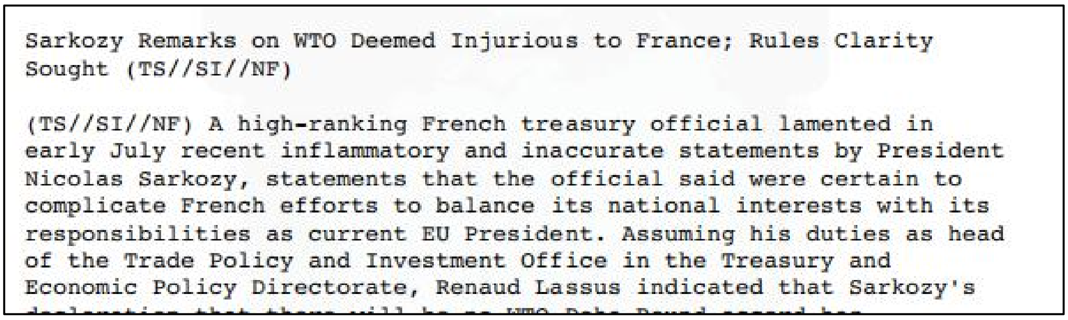
Authorized by Section 702, the U.S. intelligence agencies have established a large-scale global Internet surveillance network, offering a huge amount of high-value intelligence to the U.S. government agencies, enabling the U.S. government to take the lead in diplomacy, defense, economy, science and technology, etc. Section 702 and the accompanying Internet surveillance system have become the secret weapon of the U.S. to maintain its hegemony at this stage. With this huge first-mover technological advantage, the U.S. federal government and its intelligence agencies have become increasingly unscrupulous and any target could be on the key monitoring list. The following is a brief review with facts.

1. France

From 2004 to 2012, the U.S. conducted a long-term espionage operation against France, eavesdropping on French government policies, foreign affairs, finance, international exchange, infrastructure construction, commercial and trade activities. Some of the vital intelligence was authorized by the U.S. to be shared with the other Five Eyes partner countries, which indicated that the Five Eyes countries were also beneficiaries of the U.S. espionage operations. The surveillance records included phone calls from France's core political and economic departments, as well as phone calls at the official residence of the French president. Publicly disclosed classified U.S. intelligence documents contain a number of top-secret intelligence summaries stolen by eavesdropping on conversations and communications from senior French government officials, including the former French president (as shown in Figure 15), finance minister, foreign minister, senators, French ambassador to the U.S., and officials responsible for EU trade policy.

The intelligence covered French government's policies and internal considerations regarding the World Trade Organization, Trans-Pacific Partnership Agreement, G7 and G20, as well as France's financial budget, decline of the French automobile industry, and the participation of French companies in the Oil-for-Food program in Iraq, etc.

In the economic espionage order, the U.S. explicitly required that information should be collected on the sale and financing of all major projects in France related to telecommunications, electricity, gas, oil, nuclear and renewable energy, as well as environmental and medical technology. It also required the interception (theft) of every contract or transaction of a French company worth more than US$200 million, with a direct impact on large French companies such as BNP Paribas, AXA, Credit Agricole, Peugeot, Renault, Total, and Orange, as well as the main agricultural associations. A summary of some of the intelligence captured by the NSA in its espionage operations against France is show in Table 1.



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

Figure 15 The NSA's surveillance transcript of former French President Nicolas Sarkozy

Year/Date	Intelligence Type	Intelligence Content
2004	Intelligence on the French ambassador to Washington	The French ambassador to Washington intends to release a list of U.S. companies purportedly benefiting from the Oil-for-Food program.
2006	Intelligence on correspondence among senior French government officials	The then French President Jacques Chirac and French Minister of Europe and Foreign Affairs discuss matters on UN appointments.

Year/Date	Intelligence Type	Intelligence Content
2008	Intelligence on correspondence among senior French government officials	The head of the French finance and economic policy bureau is dissatisfied with the remarks of the then French President Nicolas Sarkozy on the potential negative impact of a WTO agreement on France.
2008	Intelligence on correspondence among senior French government officials	The then French President Sarkozy blames global economic crisis on the U.S. Government, saying that France will take the lead in pursuing transformation of the world financial system.
March 24, 2010	Intelligence on correspondence among senior French government officials	Dialogue between the French ambassador to Washington and the advisor to the French president on foreign affairs: The then French President Sarkozy plans to put forward some sensitive topics during his meeting with the then U.S. President Barack Obama in Washington on March 31, 2010. These topics involves the U.S. withdrawal from the bilateral intelligence cooperation agreement (the agreement may constrain the U.S. ability to continue monitoring France), and the likely promise of France on offering military training aircraft to Afghanistan; a possible contract on refueling aircraft between the European Aeronautic Defense And Space Company (EADS) and the U.S. military; the trademark dispute involving French spirit company Pernod Ricard.

Year/Date	Intelligence Type	Intelligence Content
June 10, 2011	Intelligence on correspondence among senior French government officials	Dialogue between the then French President Sarkozy and French Minister of Europe and Foreign Affairs: Sarkozy makes strong statement on the Israeli-Palestinian issue.
August 2, 2011	Intelligence on correspondence among senior French government officials	Dialogue among French and EU officials in Washington: They are highly critical of the U.S. trade policies, saying that the TPP is targeted at China.
May 22, 2012	Intelligence on correspondence among senior French government officials	The French government is concerned about the impact of the continuing eurozone crisis, particularly the Greek withdrawal from the eurozone, on the interest of France and French companies. The then French President Francǫis Hollande is dissatisfied with the then German Chancellor Angela Merkel's uncompromising stance on the crisis. Sarkozy agrees to the holding of a secret meeting among French officials and German opposition party members to discuss crisis without informing Merkel.
July 31, 2012	Intelligence on correspondence among senior French government officials	Dialogue between the French economy and finance minister and a senator: The minister states that the French economy has been in crisis and is expected to be in a dire situation in the following two years.

Year/Date	Intelligence Type	Intelligence Content
2012	The U.S. espionage order targeting France	The order requires engaging in long-term economic espionage to obtain details on the economic activities of French companies and the economic policies and decisions of the French government. It also involves issues such as the economic relationship of France with the U.S., other countries and international agencies, French financial and trade policies, and the French perspective on G8 and G20 agendas.
2012	The U.S. espionage order on French economy	The order instructs U.S. spies to collect sales and financing information of all major French projects relating to telecommunication, power generation, natural gas, petroleum, nuclear energy and renewable energy, as well as environment and medical technology. Meanwhile, the spies are asked to intercept and report to the higher body all contracts and negotiations of French companies that worth more than $200 million. Related intelligence will be submitted to U.S. trade, political and intelligence agencies.
2012	Intelligence on agendas of meetings among French government officials	The French Economy and Finance Ministry drafted talking points for G7 and G20 meetings, including urging the U.S. banking reform, and planning to support the U.S. on the strategic petroleum reserve initiative.

Table 1 The NSA’s surveillance records of French government officials in office at the time

2. Germany

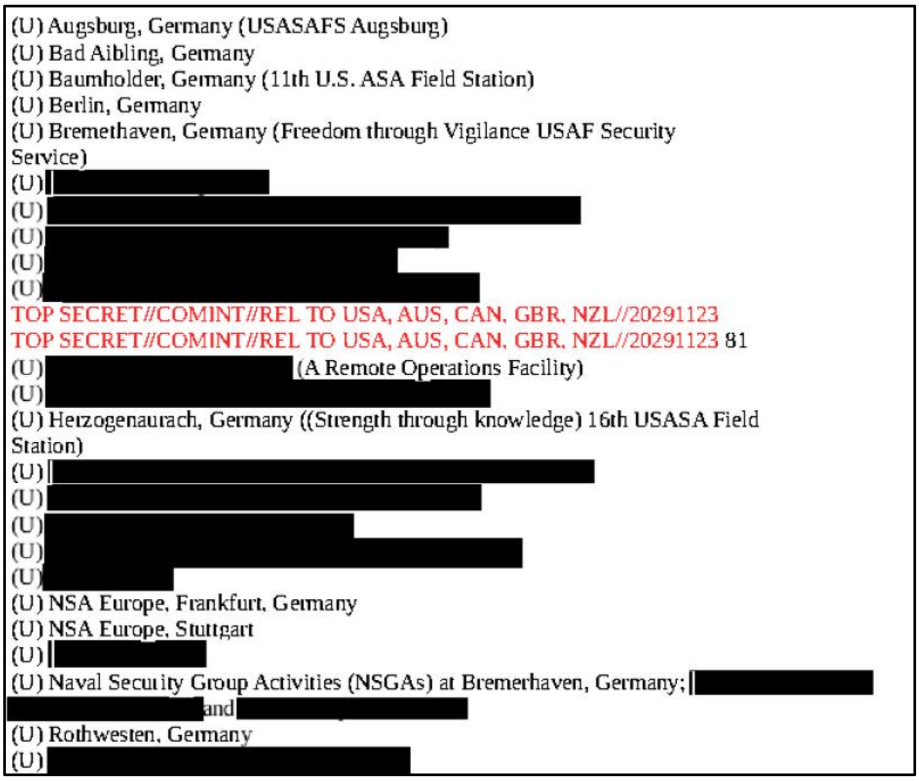
An NSA confidential document shows that the Germany Federal Intelligence Service (BND) and the Federal Office for the Protection of the Constitution (BfV) and other intelligence agencies have provided active cooperation for their U.S. counterparts several times to conduct surveillance activities in Europe and Germany itself.[3] They also joined hands with the CIA in acquiring and operating the Switzerland-based encryption technology company Crypto AG, and offered encryption products with backdoor to the targets of surveillance.[4] In spite of that, the U.S. has excluded Germany from the Five Eyes, and categorized Germany as a third-tier partner, regarding Germany as both a partner of interests and an untrustworthy target of surveillance.

In fact, the U.S. Army, Air Force, and Navy,

[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

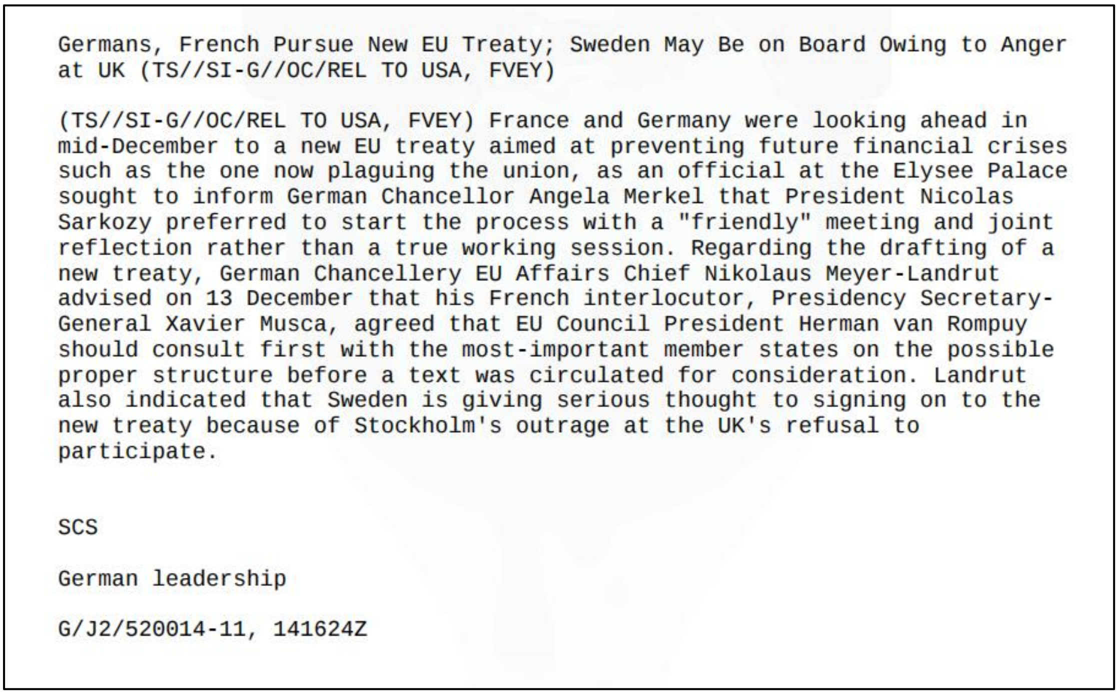
as well as the NSA have set up a large number of covert intelligence stations in Germany to keep close watch on Germany and other European countries (as shown in Figure 16).



(U) Augsburg, Germany (USASAFS Augsburg)
(U) Bad Aibling, Germany
(U) Baumholder, Germany (11th U.S. ASA Field Station)
(U) Berlin, Germany
(U) Bremerhaven, 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]

Figure 16 Covert intelligence stations set up in Germany by the U.S. intelligence agencies

The NSA has long been monitoring correspondence among senior German government officials, including chancellors, ministers of foreign affairs, ambassadors and consul- generals abroad. The surveillance content is extensive, including the German government’s perspective on the international situation and emergencies, as well as private discussions among Germany officials after they attend international exchanges with the U.S., covering such important fields as politics, military affairs, economy, diplomacy, policy, ethnicity, security, resources, etc. What’s worth mentioning is that the U.S. intelligence agencies have a keen interest in the internal considerations of EU countries, especially their solutions to guarding against financial risks (as shown in Figure 17).



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

Figure 17 The NSA surveillance records of German government leaders

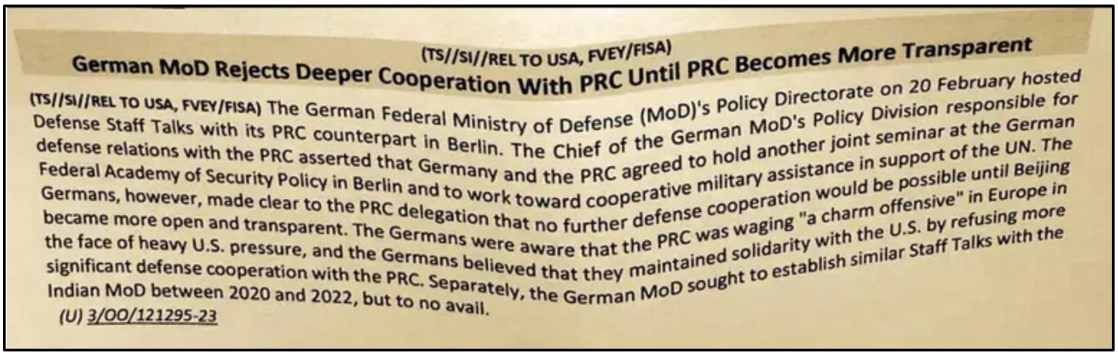
Even after the Snowden leaks, the U.S. has not relaxed its surveillance on Germany. It has done so with a more covert approach. In May 2021, Danish media[5] exposed the cooperation between the NSA and the Danish Defense Intelligence Service (FE) on monitoring Internet cables in Denmark. The targets included state leaders, as well as senior politicians and officials of Germany, Sweden, Norway, and France. The then German Chancellor Angela Merkel, then

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

German Minister of Foreign Affairs Frank-Walter Steinmeier and then Germany opposition leader Peer Steinbruck, to name a few, were all main targets of the surveillance project between the NSA and the FE. The person in charge of the project happened to be the then U.S. Vice President Joe Biden, who is currently the U.S. President.

The exposure of the project once again aroused dissatisfaction of Germany, France, and other European countries. The then German Chancellor Merkel and French President Emmanuel Macron had publicly stated that the U.S. surveillance targeting its allies was "unacceptable." However, the U.S. was obviously indifferent to the feeling of its "allies." In April 2023, the U.S. surveillance targeting German Federal Ministry of Defense was exposed again.[6]

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



(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

Figure 18 The NSA’s surveillance records of the German Federal Ministry of Defense

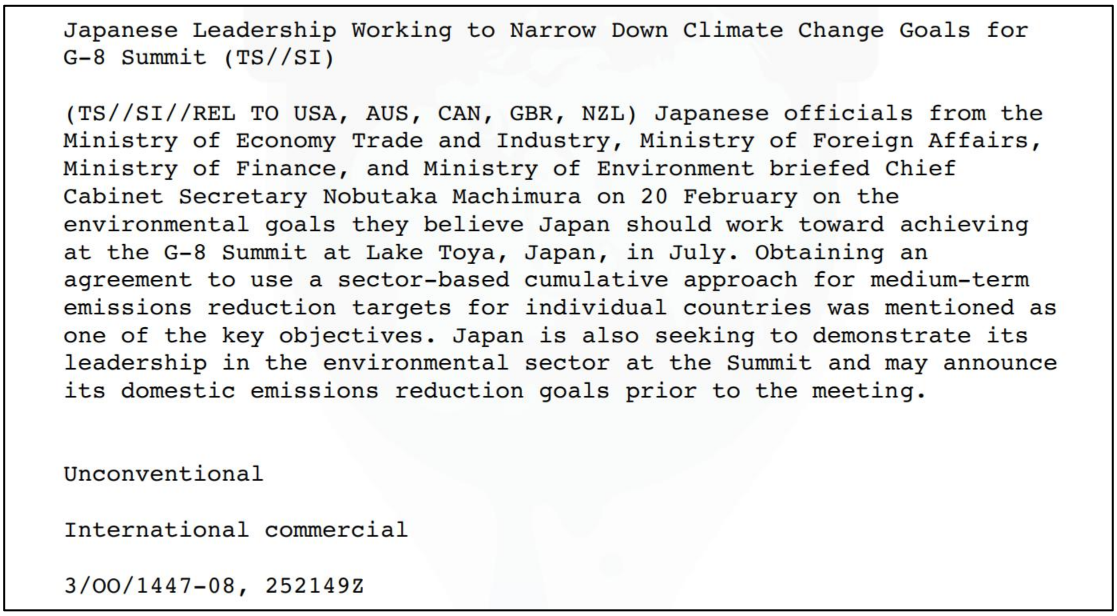
The NSA top-secret document (as shown in Figure 18) shows that the activity monitored this time was the meeting on military and foreign affairs between the German Federal Ministry of Defense and a visiting delegation of the Ministry of National Defense of China on February 20, 2023. The records revealed that the main focus of the U.S. was the views and stance of Germany on military cooperation with China.

In 2022, the U.S. and Europe have established a new “U.S.-EU Trans-Atlantic Data Privacy Framework”, and the United States promised to give more supervision of cyber surveillance operation in Europe for tricking the so-called allies into agreeing to transmit data to the United States. In fact, the US has never stopped wiretapping its European Allies.

3. Japan

The external surveillance database of the NSA included a list of important Japanese political and economic targets. The list showed that the NSA espionage monitoring activities targeting the Japanese cabinet, government departments and zaibatsus could be traced back to the Shinzo Abe administration. Phone surveillance targets included the office switchboard of the Japanese cabinet, executive secretary of the then chief cabinet secretary Yoshihide Suga, a large number of Japanese central bank officials, the natural gas department of the Mitsubishi Corp., and the petroleum department of the Mitsui & Co. Machine Tech Ltd. A record titled “A Confidential Proposal on Climate Change that Japan Plans to Release at the

G8 Summit" (as shown in Figure 19) clearly marked "REL TO USA, AUS, CAN, GBR, NZL," meaning that the intelligence report was officially approved by the senior U.S. government authority to be shared with the Five Eye allies, creating conditions for them to come up with special plans targeting Japan. Relevant intelligence was suspected to be stolen from Japanese government agencies, which further demonstrated the extensive coverage of the U.S. government surveillance targeting its Japanese counterpart. Specific contents of concern were: disputes on agricultural product imports and trade, Japan's stance at the WTO Doha Development Round, Japan's climate change policies, its nuclear energy and energy policies and carbon emission plans, correspondence between Japan and international agencies such as the International Energy Agency, the prime minister's briefings at Shinzo Abe's official residence, and much more.



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

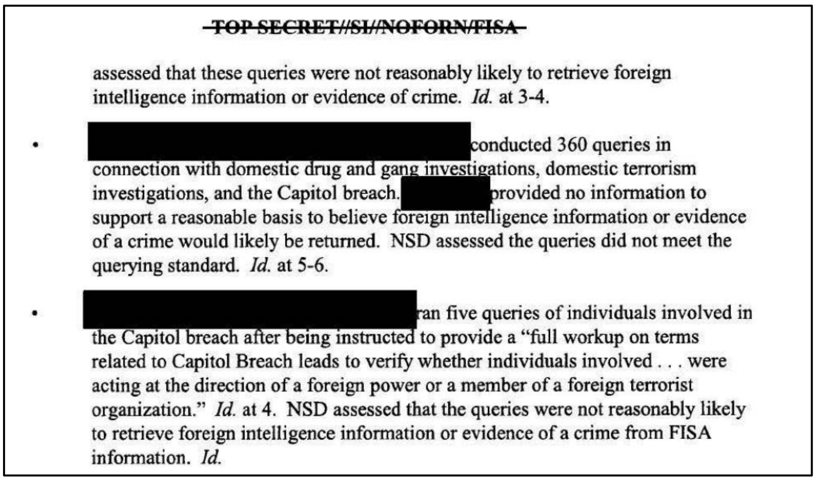
Figure 19 The NSA’s monitoring records of Japanese leaders

4. Ordinary U.S. Citizens

Our second investigation report has made it clear that there has been a public outcry of justice against Section 702. Although the section claimed that the U.S. intelligence agencies such as the NSA only collect information from overseas non-American, obviously, the overall mission of such monitoring plans is to illegally obtain full information data of global Internet users, as shown in the aforementioned technical route of the NSA surveillance plans. The targets absolutely include U.S. citizens. When intelligence analysts set selectors, they are asked by the NSA and the rest of the U.S. intelligence community to "try to" avoid covering U.S. citizens at home and U.S. citizens abroad. But unfortunately, such measures that rely almost entirely on "self-discipline" are merely symbolic. On May 19, 2023, the U.S. Foreign Intelligence Surveillance Court publicly released a document,[7] showing that the U.S. intelligence community had carried out thousands of operations that violated Section 702 (as shown in Figure 20). The document particularly pointed out that when the FBI collected foreign intelligence, it repeatedly misused telecommunication and online surveillance tools, including monitoring U.S. citizens related to the Capitol riot on January 6, 2021, and the "Black Lives Matter" social movement in 2020. The court order was later

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

publicly exposed and questioned by the media.[8] As a matter of fact, during the "Occupy Wall Street" populist movement, agencies including the FBI, NSA and CIA carried out non-differentiated monitoring of on-site protesters and their contacts throughout the whole process. Similar methods were adopted during the "Sunflower" riot in China's Taiwan region and the illegal "Occupying Central" in China's Hong Kong Special Administrative Region. Thus, it can be seen that surveillance on U.S. citizens has never been absent.



~~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.

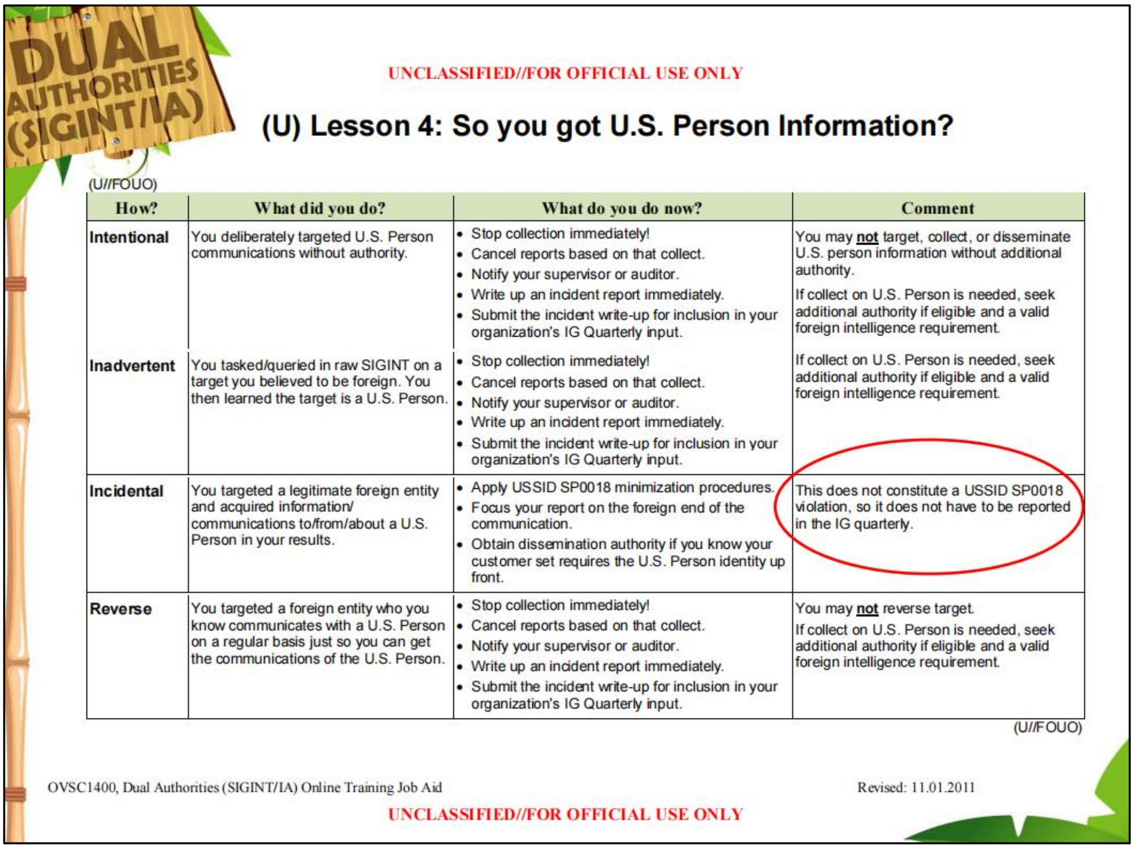
- [redacted]an five queries of individuals involved in the Capitol breach after being instructed to provide a "full workup on terms related to Capitol Breach leads to verify whether individuals involved . . . were acting at the direction of a foreign power or a member of a foreign terrorist organization." *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.*

Figure 20 Cases of Section 702 violation revealed in the U.S. Foreign Intelligence

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

Surveillance Court document

The underlying reason of such Internet surveillance misuse is that the U.S. intelligence community has adopted an excessively lenient attitude in enforcing Section 702 (as shown in Figure 21). Intelligence agencies have even made it clear in their internal training materials that if intelligence analysts “accidentally” find personal information of U.S. citizens, it is not a violation of rules and it’s not necessary to report.


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

Figure 21 Training material of the U.S. intelligence community on Section 702 compliance requirements

The aforementioned examples demonstrate that the U.S. global online surveillance plan and monitoring stations are like ubiquitous lurkers on the Internet, which eavesdrop and steal data from online users all over the world in real time. Such surveillance capacity is an indispensable foundation for the U.S. to build a Matrix and espionage empire. To maintain such a large surveillance plan requires an astonishing annual budget. The need for more budget comes with the explosive growth of online data. That is the main driving force for the U.S. federal government and intelligence community to jointly push for the planning and development of Volt Typhoon.

It is not a rare case for U.S. politicians to cheat the U.S. Congress for their personal gains. The FBI Director Christopher Wray, who has played an important role in the Volt Typhoon false narrative campaign, is a habitual liar. In July 2022, Wray and the U.S. Attorney General Merrick Garland were questioned by senators for covering up the evidence of crime by President Biden's son.[9] In August 2023, Wray faced questions by several Congress members for submitting fake memo to Congress.[10] In July 2024, Wray, again, perjured himself at a House hearing on the

[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/

shooting of former U.S. President Donald Trump when he claimed that Trump wasn't hit by a bullet,[11] while concealing the real health condition of the current President Biden. For that matter, Trump strongly urged Wray to resign immediately.

IV. Demon behind Unusual Events

We have taken into notice that after we released the second investigation report on Volt Typhoon, although the U.S. authorities and the mainstream media kept silent, some former and current U.S. government officials and Internet security companies expressed their views on our report via social media, media of the U.S. Internet security and independent media, including a unanimous negative opinion, saying that the report "distorted" and "misused" the research outcome of relevant U.S. companies. The U.S.

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

companies were also eager to disassociate themselves with the report. Therefore, we feel that it’s necessary to point out that in investigation and research of cyberattack incidents, citing and referring to research results of other professional agencies is nothing new but a normal practice. Being considered “distorting” and “misusing” the results of some U.S. companies just because we came up with different conclusions made us realize the power of U.S. Internet hegemony. It also made us believe that these companies had expressed their view under tremendous external pressure.

ThreatMon’s change of statement is quite intriguing. It claimed during a media interview that it revised the original report because it found out in its follow-up research mistakes in the early indicators of compromise related to the Volt Typhoon investigation report. Such perfunctory explanation makes it even more suspicious. For one thing, the time it revised the report raises doubts; for another, the entire page deleted from the original report not only included an IP address list, but key evidence such as command and control server addresses and ransomware cryptocurrency wallet addresses. Is it possible that these data all went wrong during the collection process? What has happened to ThreatMon's scientific research attitude, technical expertise and competence? Is it ThreatMon's academic spirit to strictly keep its report the same as the reports of other obedient U.S. Internet security agencies under the pressure of U.S. authorities? If the follow-up research was thorough and rigorous, why didn't ThreatMon provide an explanation in the revised version and revise the content page accordingly? The only explanation for ThreatMon's fishy move is that the original report was changed in a rush due to strong external pressure. Of course, we have already presented in our latest report more evidence, which can fully prove the Internet espionage that the U.S. intelligence community has conducted on China, Russia, Iran and Arab countries, as well as the fact that fake information has been given to the U.S. Congress and tax payers.

The response from Microsoft is worth noting, too. During the BlackHat USA 2024 on August 11, Sherrod DeGrippo, Director of Microsoft’s Threat Intelligence Strategy, said that the so-called “Volt Typhoon” was still active with no signs to stop. However, she failed to provide concrete evidence of Volt Typhoon as a so-called “Chinese government-sponsored cyber actor.” As a matter of fact, the behavior of Microsoft has been suspicious since 2023. It has strengthened cooperation with the U.S. military and intelligence community, as we pointed out in the previous two reports. The cooperation has gone further in 2024. According to an article published on Bloomberg on May 7,[12] Microsoft has deployed an offline AI large model and assistant program for U.S. intelligence agencies to conduct auxiliary analysis of top-secret information. What's more worrying is the excessive attention Microsoft has paid to the private information of its users. On May 21, the company released the new AI solution Copilot+ PCs and the "Recall" feature, with which the Windows operating system is able to record every user operation for its AI assistant to learn. Although Microsoft explained that the feature is only limited to local operation, and the data are stored in an encrypted form, users' doubts about the misuse of Recall and leakage of personal information cannot be dispelled. Overwhelmed by the massive controversy, Microsoft had to postpone the Recall feature that should have been pushed with

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

Windows updates. On June 13, OpenAI, of which Microsoft is the largest stakeholder, appointed Paul Nakasone to its board of directors. All of these moves by Microsoft fully indicate that the company, as a crucial partner of the Section 702-related surveillance project, has been increasingly influenced and controlled by the U.S. intelligence community. In return, the U.S. government agencies have turned a blind eye to Microsoft’s disguised monopolistic behaviors –abusing its dominant market position and using Windows and Office updates to push bundled software products.

Here, we must mention the famous U.S. cybersecurity firm CrowdStrike’s update flaw on July 19, which caused the Blue Screen of Death on millions of computers installed with the Windows operating system. The accident also led to serious losses of public transportation, health care and other key information infrastructure industries for a number of countries. Such an accident is not what global cybersecurity practitioners would like to see. Particularly, for professionals in the field of computer virus prevention and control, such incident will definitely deal a heavy blow to user confidence in third-party antivirus programs, and further affect the ecosystem of the global Internet security industry. Nevertheless, facing such a serious accident, the Cybersecurity and Infrastructure Security Agency (CISA), as the main cybersecurity authority of the U.S., showed abnormal “leniency” to Microsoft and CrowdStrike. The CISA did not take any action. Instead, its director Jen Easterly called the accident a “dress rehearsal” for Volt Typhoon attacks at the BlackHat USA 2024, actively absolving Microsoft and CrowdStrike from their blame and diverting public attention. These nonsensical and shameless statements and actions have profound underlying reasons. In fact, the accident demonstrated the significant advantage of the U.S. in the IT supply chain. As important partners of the U.S. intelligence community, Microsoft and CrowdStrike were surely able to receive “protection” from the U.S. government agencies. They would not be punished. On the contrary, under the shelter of the authorities and the disguise of the so-called “China cyber threat,” they would continue to expand their influence on the global market and deliver more information to the Section 702 database.

In the meantime, we have also noticed that many well-known media, international figures and industrial experts from America, Europe, Asia and Africa have raised voices of justice on the truth of Volt Typhoon. Notably, an Australian expert published a feature commentary article title *The Geopolitics of Cyber Espionage*,[13]

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

clearly pointing out that the U.S. government and Microsoft reports lack concrete evidence, and revealing that "the Volt Typhoon threat was mostly a work of fiction, crafted by U.S. intelligence agencies to win public support and pressure policymakers to allow the extension of invasive U.S. surveillance powers." We would like to express our sincere appreciation for their outspoken advocacy of justice.

V. Conclusion

For years, the U.S. federal government, out its selfish interest, has turned the tracing of cyberattacks the into a political issue. To cater to U.S. politicians, government bodies and intelligence agencies, some U.S. companies, such as Microsoft and CrowdStrike, for their commercial interest and without sufficient evidence and rigorous technical analysis, have been keen on coining various absurd code names with obvious geopolitical overtones for hacker groups, such as “typhoon,” “panda,” and “dragon,” instead of “Anglo-Saxon,” “hurricane,” and “koala.” They flaunted their “superb” skills and cultural “deposits,” but ignored the most basic issue of product quality, corrupting the overall culture of the industry. We have reiterated multiple times in our previous reports that China has always been opposing technical investigation of cybersecurity incidents manipulated by political games and the politicization of the tracing of cyberattacks. On the contrary, the U.S. federal government has been persistently inciting and abetting from the shadow, fabricating fictitious cyberattacks to scam for budget from Congress. As its ambitions grow larger, it is bound to shoot itself in the foot one day. Wray and other unethical politicians, who have been utilizing the Volt Typhoon deceptive narrative to cheat the U.S. Congress and public and obtain illicit gains, are destined to face a just judgment from the American people.

Against the backdrop of today's increasingly intense geopolitical conflicts, normalized international exchange is what the cybersecurity industry needs the most. Again, we would like to call for extensive international collaboration in this field. Moreover, cybersecurity companies and research institutions should focus on counter-cyber threat technology research and better products and services for users. That is the right way forward for the Internet to contribute steadily to the common progress of mankind.

National Computer Virus Emergency Response Center

National Engineering Laboratory for Computer Virus Prevention Technology

October 14, 2024