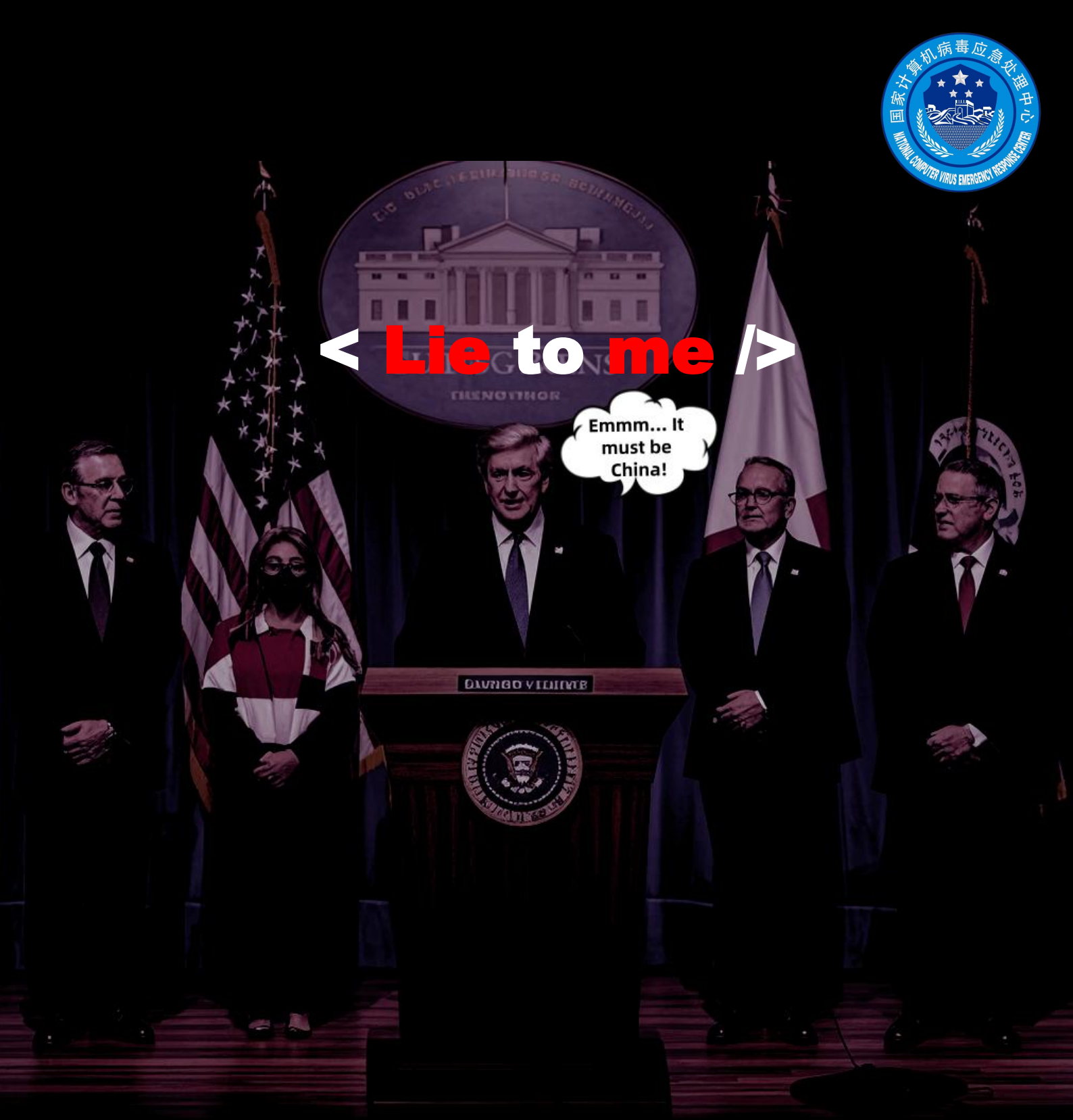


Volt Typhoon III

— Enthüllung der Cyberspionage und Desinformationskampagne von den US-Regierungsbehörden

Abstract: Nach der Veröffentlichung der ersten beiden Untersuchungsberichte über den sogenannten „Volt Typhoon“ verhielten sich US-Regierungsstellen, Mainstream-Medien und das Unternehmen Microsoft gemeinsam schweigend. Doch die ehemaligen und amtierenden Beamten der US-Geheimdienste und der US-Cybersicherheitsbehörden, vertreten durch Robert Joyce, äußerten sich eifrig dazu. Anstatt auf die zuvor bekanntgemachten Beweise von chinesischer Seite zu verweisen, rechtfertigten sie sich mit Ausflüchten. Das gilt ebenfalls auch für einige US-amerikanische Unternehmen und Medien auf Gebiet Cybersicherheit. All dies legt wieder einmal ihr wahres Gesicht an den Tag, sprich: Wer ein schlechtes Gewissen hat, reagiert empfindlich oder stiftet Konfusion, um den Verdacht von sich abzulenken. Basierend auf unseren beiden vorangegangenen Berichten geht es bei der neuen Berichtsversion darum, die von der US-Bundesregierung, den Geheimdiensten und der „Five Eyes“-Allianz implementierten Online-Spionageaktivitäten, -Lauschangriffe und -Abhörmaßnahmen gegen Länder wie China und Deutschland, aber auch globale Internetnutzer, noch weiter unter Beweis zu stellen. Noch geklärt sind darin auch unbestrittene Belege,

wie sie durch unsichtbare „Toolkits“, die Rückverfolgungs- und Attributionsanalyse irreführend machen, Operationen unter „Falscher Flagge“ zur Vertuschung eigener bösartiger Cyberangriffe durchführen und die Schuld auf andere Länder schieben. Hinzu kommt die Enthüllung der Tatsache, dass die Vereinigten Staaten Angriffe mittels Lieferketten übernehmen, Hintertüren in Internetprodukten einbauen und „Pre-Position“ einsetzen. Unser Anspruch ist deswegen, die politische Farce im Namen „Volt Typhoon“, die von der US-Bundesregierung selbst erfunden und inszeniert wird, gründlich zu entlarven.

1. Einleitung

Am 15. April und 8. Juli 2024 veröffentlichten das National Computer Virus Emergency Response Center (CVERC), das National Engineering Laboratory for Computer Virus Prevention Technology und die 360 Digital Security Group zwei Themenberichte, und zwar jeweils mit dem Titel *Volt Typhoon: Eine konspirative Betrugskampagne gegen den US-Kongress und die Steuerzahler durch die US-Geheimdienste*[1] und *Volt Typhoon II: Eine geheime Desinformationskampagne gegen den US-Kongress*

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

und die Steuerzahler durch die US-Regierungsbehörden[2]. In aller Hinsicht wird darin aufgedeckt, dass die US-Regierungsbehörden globalen Telekommunikation und Internetnutzer wahllosem Abhören aussetzen lassen, um die sogenannte „Überwachungsbefugnis ohne richterliche Anordnung“ weiterhin in der Hand zu halten. Die zwei Papiere machen auch klar, dass die US-Regierungsbehörden Cyber-Bedrohungen aus China erfunden haben. Ihr Ziel ist, größere politische und wirtschaftliche Interessen für die entsprechenden Interessengruppen, die hinter den USA stehen, zu erzielen. Ihr Vorgehen erweist sich nichts anderes als eine Posse im Stil von „House of Cards“, wobei die Mitglieder des US-Kongresses und die Steuerzahler aufs Kreuz gelegt wurden. Nach der Bekanntgabe der Berichte reagierten die Lügner, die United States Agency for Global Medie sowie die von ihr manipulierten US-amerikanischen und westlichen Mainstream-Medien nach wie vor schweigend, jedoch sorgte ihre diese Haltung in der globalen Gemeinschaft für große Aufmerksamkeit. Mehr als 50 Cybersicherheitsexperten aus Europa und Asien, wenn nicht sogar ja aus den Vereinigten Staaten, wendeten sich auf verschiedene Weise an uns. Sie sind der Meinung,

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

dass es in die Vorgehensweise von den USA und Microsoft, den „Volt Typhoon“ mit der chinesischen Regierung in Verbindung zu bringen, stichhaltige Argumentation mangle. Zugleich äußerten sie sich besorgt über die Manipulation der Fiktion von „Volt Typhoon“ durch die USA. Parallel dazu ermöglicht es die zunehmende Aufmerksamkeit diesbezüglicher Themen im Internet der internationalen Gemeinschaft, sich dem wahren Gesicht der Vereinigten Staaten und ihrer Cyber-Hegemonie noch weiter näherzubringen. Hiermit könnte die globale Gemeinschaft sich Einsicht auf die reale Gefahr verschaffen, die die USA mittels des Internets die ganze Welt dem Abhören undifferenziert unterziehen. In diesem Zusammenhang ist es vonnöten, mehr objektive Nachweise in Bezug auf die Erfindung der „Volt Typhoon“-Fiktion, die Organisation und Durchführung von Operationen unter „Falscher Flagge“ und die Cyberangriffe gegen China durch die US-Regierungsbehörden offenzulegen. Wir fühlen uns verpflichtet, ihre Intrigen noch intensiver frei zu machen.

2. Das „Chamäleon“ im Cyberspace

Es ist allgemein bekannt, dass die USA der weltweit größte Waffenlieferant sind, gepaart mit einem großen

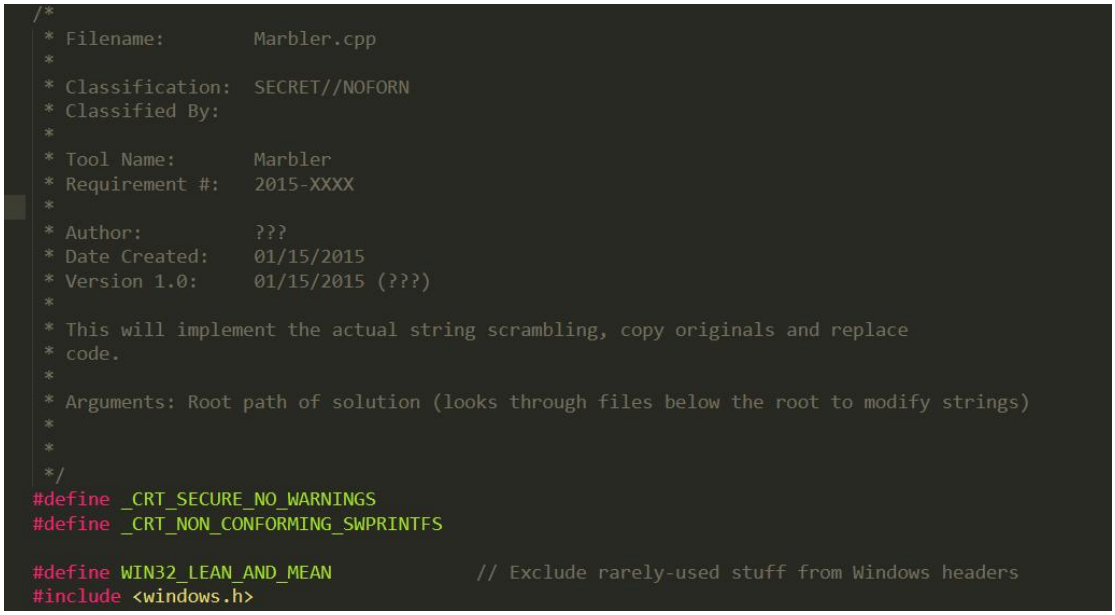
militärisch-industriellen System und einem dazugehörigen starken Komplex. Beide bilden einen wichtigen Eckpfeiler, der über Politiken des Landes in Politik, Wirtschaft und Militär Herr ist. Daraus entsteht ein umfangreiches Cyberwaffenarsenal, das sich durch vielfältige Formen und eine reiche Palette mit komplexen Funktionen auszeichnet. Das CVERC hat zuvor schon eine Reihe von Cyberwaffen, die von der National Security Agency (NSA) und der Central Intelligence Agency (CIA) der USA entwickelt wurden, der Öffentlichkeit vorgestellt. In dem Untersuchungsbericht über die Cyberangriffe der NSA gegen die Northwestern Polytechnical University wurden die Funktionen mehrerer Cyberwaffen, die von den zuständigen US-Geheimdiensten bei ausländischen Cyberangriffen eingesetzt wurden, unter die Lupe genommen. Ans Licht gebracht wurden überdies die bei den hochgradig verdeckten Angriffen verwendeten Techniken und Taktiken. Aber: All dies entpuppt sich nur als die „Spitze des Eisbergs“ des riesigen Cyber-Arsenals des US-amerikanischen „Hacker-Imperiums“.

Seit langem verfolgen die USA aktiv die Strategie der „Vorneverteidigung“ und führen die taktische Operation der „Hunt-Forward“ im Cyberspace durch. Es heißt also, dass sie

Streitkräfte für Cyber-Kämpfe rund um gegnerische Länder anordnen, und zwar mit dem Ziel, deren Online-Ziele so nah wie möglich dran zu ermitteln und zu infiltrieren. Um diesem taktischen Bedarf gerecht zu werden, haben die US-Geheimdienste eigens ein unsichtbares „Toolkit“ mit dem Tarnamen „Marble“ entwickelt. Mit diesem Komplex pochen sie darauf, ihre eigenen bösartigen Cyberangriffe zu verschleiern, die Schuld auf andere Länder zu schieben sowie Rückverfolgungs- und Attributionsanalyse in die Irre zu führen. Bei dem Toolkit handelt es sich um einen Rahmen von Werkzeugen, die in andere Projekte zur Entwicklung von Cyberwaffen integriert werden können. Es unterstützt Entwickler von Cyberwaffen dabei, verschiedene identifizierbare Merkmale der Programmcodes zu verwechseln. Dadurch werden die „Fingerabdrücke“ der Entwickler effektiv „gelöscht“, ähnlich wie Veränderung der „Züge“ einer „Feuerwaffe“. Mit der unkorrekten Ausrichtung macht es den Ermittlern unmöglich, die wahre Herkunft der Waffen aus technischer Sicht zurückzuverfolgen. Des Weiteren ist das Framework mit einer „schamloseren“ Funktion behaftet, nämlich die Möglichkeit, nach Belieben Zeichenketten in anderen Sprachen wie Chinesisch, Russisch, Koreanisch, Persisch und

Arabisch einzufügen. Das Ziel ist auch offensichtlich, den Ermittlern an der Nase herumzuführen und damit letztendlich China, Russland, Nordkorea, den Iran und mehrere arabische Länder zu beschuldigen.

Aus dem Marble-Quellcode und seinen Kommentaren (vgl. Abbildung 1) geht hervor, dass es sich um ein als geheim eingestuftes (und darf nicht für das Ausland bekanntgegeben) Waffenentwicklungsprogramm handelt, das spätestens im Jahr 2015 auf den Weg gebracht wurde. Kein Wunder also, dass das Programm als eine „Geheimwaffe“ dient, die die US-Geheimdienste für sich selbst maßgeschneidern. Selbst lassen sie ihre sogenannten „Verbündeten“ darüber im Unklaren.



```
/*
 * 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>
```

Abbildung 1: Marble-Quellcode

Mehr als 100 Verwirrungsalgorithmen können es dem Marble-Framework erlauben, lesbare Variablennamen und Zeichenketten in Dateien mit Quellcode durch unlesbare (unerkennbare) Inhalte zu ersetzen sowie spezifische Störungszeichenfolgen einzufügen (vgl. Abbildung 2, 3, 4 und 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
*/
```

Abbildung 2: Verwirrungsfunktion

```
#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"
```

Abbildung 3: Verwirrungsalgorismus

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

Abbildung 4: Funktion zur Dokumentenbearbeitung

```
    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;
                }
```

Abbildung 5: Funktion zur Dokumentenbearbeitung (Fortsetzung)

Es kann sogar sein, dass man absichtlich eingefügte Zeichenketten in „Fremdsprachen“ aus dem Quellcode der Marble-Testbeispiele herausfindet. Zu den sogenannten „Fremdsprachen“ zählen ausschließlich Arabisch, Chinesisch, Russisch, Koreanisch und

Persisch (vgl. Abbildung 6) .

```
//Add foreign languages
//Arabic
WARBLE wcArabic[] = L" [illegible]
sb.Append((LPBYTE)wcArabic, 380);

//Chinese
WARBLE wcChinese[] = L"洴汭沘 烕煓瑚 鹿榙榾 蹖 鑴鑤, 鶑黮齵 逯郹頔萑滮 潷濾漇 麖 踶輵 泮絮涹 螨螈謕 崞愊惵 榼 趏跮, 嵥 垡婖 蟷蠉蟞 鍹
sb.Append((LPBYTE)wcChinese, 266);

//Russian
WARBLE wcRussian[] = L"Зыд нэ нонюмэш контынтёонэж. Видэ бландит ан квуй, дуо декам эпикюре эа. Йн дйкит мольлиз дэльякатезш
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" [illegible] Lorem ipsum) [illegible]
sb.Append((LPBYTE)wcFarsi, 1710);

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

return;
```

Abbildung 6: „Fremdsprachen“ in Dokumente eingefügt

Das Marble-Framework bringt also die undifferenzierten und grenzlosen Cyberspionageaktivitäten der US-Geheimdienste auf der ganzen Welt voll und ganz zum Vorschein. Wieder sichtbar sind auch ihre Tricks, durch Operationen unter „Falscher Flagge“ Ermittler und Forscher zu täuschen und „Gegner“ zum Sündenbock zu machen.

Nicht nur Code-Merkmale werden bei solchen Operationen unter „Falsche Flagge“ ins Visier genommen. Wie es in unserem zweiten Bericht ausgeführt wurde, gestatten clevere Nachahmungen der Angriffstechniken und -taktiken von Cyberkriminellen den US-Geheimdiensten, verschiedenste perfekte

„Taschen-Organisationen“ zu erfinden. In diesem Sinne tarnen die Hacker der US-Streitkräfte für Cyberkriege und Geheimdienste so geschickt wie Chamäleon, dass sie ihre Identität und ihr Erscheinungsbild im Cyberspace willkürlich wechseln. Somit starten sie im Namen anderer Länder globale Cyberangriffe zur Spionage und schwärzen Länder, die keine „Verbündeten“ der USA sind, an.

Zuverlässigen Informationsquellen zufolge sind Aktionen unter „Falsche Flagge“ de fato ein wichtiger Teil von der „EFFECTS“-Aktion der US-Geheimdienste (im Vereinigten Königreich als „Online Covert Action“ bekannt). Geheime Dokumente der Vereinigten Staaten und anderer „Five-Eyes“-Länder legt nahe, dass „EFFECTS“ aus zwei Strategien besteht, nämlich „Operation über Desinformationen“ und „Technischer Störung“, für den Letzterer steht noch ein Implementierungshandbuch zur Verfügung, das von NSA eigens erstellt wurde. In dem Handbuch sind Operationen unter „Falscher Flagge“ als ein wichtiger Bestandteil festgehalten. Auch heißt es in den internen Dokumenten der USA und ihrer „Five-Eyes“-Verbündeten mit aller Deutlichkeit, dass sich „„EFFECTS“ an vier Hauptprinzipien orientieren muss, also Leugnen, Stören, Diskreditieren und Täuschen. Ausgerechnet

spiegeln sich diese vier Prinzipien in allen zentralen Elementen von „Volt Typhoon“ wider (vgl. Abbildung 7 und 8) .

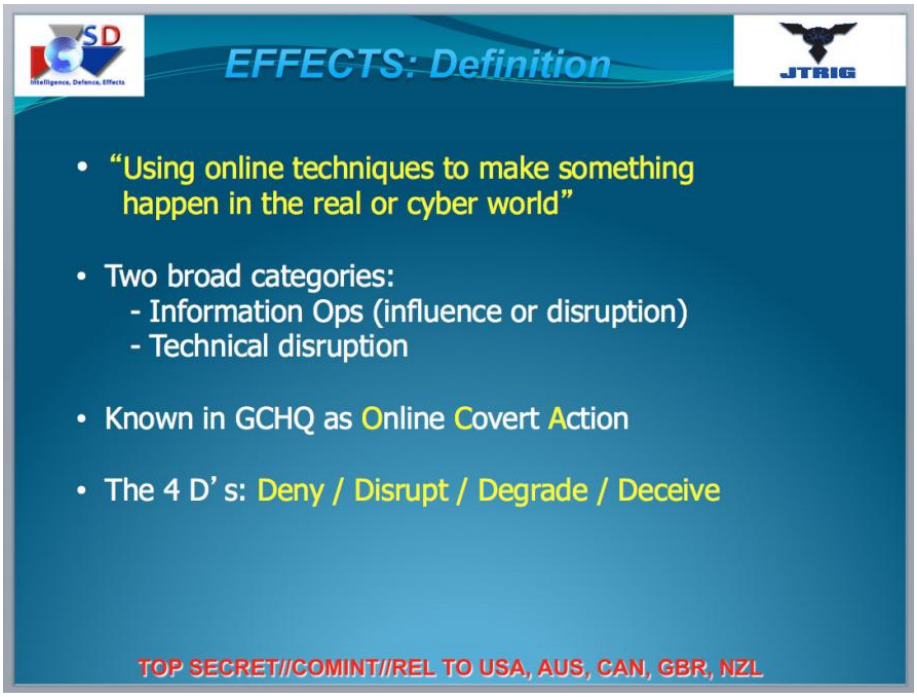


Abbildung 7: Definition der „EFFECTS“ von den USA und ihrer „Five-Eyes“-Verbündeten

Abbildung 8: Das Handbuch zur „Technischer Störung“ von den USA und ihren „Five-Eyes“-Verbündeten

Aus den obigen Beweisen lässt sich schlussfolgern, dass es bei der Aktion „Volt Typhoon“ um ein typisches und ausgetüfteltes Desinformationsmanöver geht, das im Interesse der kapitalistischen Gruppe der USA steht (auch bekannt als Operation unter „Falscher Flagge“). Dessen Techniken und Taktiken stimmen also völlig mit denen in „EFFECTS“ überein. Selbstverständlich ist es regelrecht schwer, derartigen ausgeklügelten Schwindel der nationalen US-Geheimdienste zu durchschauen. Damit dies gelingt, reicht es in Anbetracht der Großzahl von störenden Informationen bei weitem nicht aus, sich nur auf technische Analysen zu verlassen. Hierfür ist es erforderlich, Informationen aus mehreren Quellen und relevanten Materialien umfassend zu analysieren. Nur dann können die Nachlässigkeiten und Fehler, die die US-Geheimdienste versehentlich offenbaren, vor Augen geführt werden. Und nur dann kann man die miesen Finten der US-Geheimdienste wie NSA und CIA richtig verstehen und interpretieren. All das lässt sich in unseren ersten beiden Untersuchungsberichten ablesen (vgl. „Volt Typhoon: Eine konspirative Betrugskampagne gegen den US-Kongress und die Steuerzahler durch die US-Geheimdienste“ und „Volt Typhoon II:

Eine geheime Desinformationskampagne gegen den US-Kongress und die Steuerzahler durch die US-Regierungsbehörden“).

3. Der „Schnüffler“ im Cyberspace

In unserem zweiten Bericht bringen wir den politischen Skandal der US-Regierungsbehörden, insbesondere der Geheimdienste ans Tageslicht. Dem Abschnitt 702 des US Foreign Intelligence Surveillance Act (FISA) zufolge dürfen sie Menschen ohne richterliche Anordnung ausspähen. Um von dieser Überwachungsbefugnis weiterhin Gebrauch zu machen, scheuen sie keine Mühe, externe Cyberbedrohungen zu schwindeln und Desinformationskampagnen zu entfachen. Das Ziel: Ihre umfangreichen, undifferenzierten und zügellosen Abhörprogramme aufrechterhalten. Im vorliegenden Papier fokussieren wir weiterhin auf die Einzelheiten der obigen Abhörpläne.

3.1 An der „Kehle“ des Internets packen

Nach internen, streng geheimen Daten der NSA (vgl. Abbildung 9) halten die USA aufgrund ihrer technologischen und geografischen Vorteile die Schlüsselstellung, also „Kehle“ des Internets in Schach. Dazu zählen die weltweit wichtigsten Unterwasserkabel im Atlantik

und im Pazifik. Sieben staatliche Stationen zum Abhören von allen Daten sind eingerichtet worden. In enger Zusammenarbeit mit dem Federal Bureau of Investugation (FBI) und dem National Cyber Security Centre (NCSC) des Vereinigten Königreichs unternimmt das Land eine tiefgründige Protokollanalyse und einen Datenklau der gesamten über Glasfaserkabel übertragenen Datenmenge. Auf dieser Weise ist dann ein wahlloses Ausspähen von weltweiten Internetnutzern in Sicht.

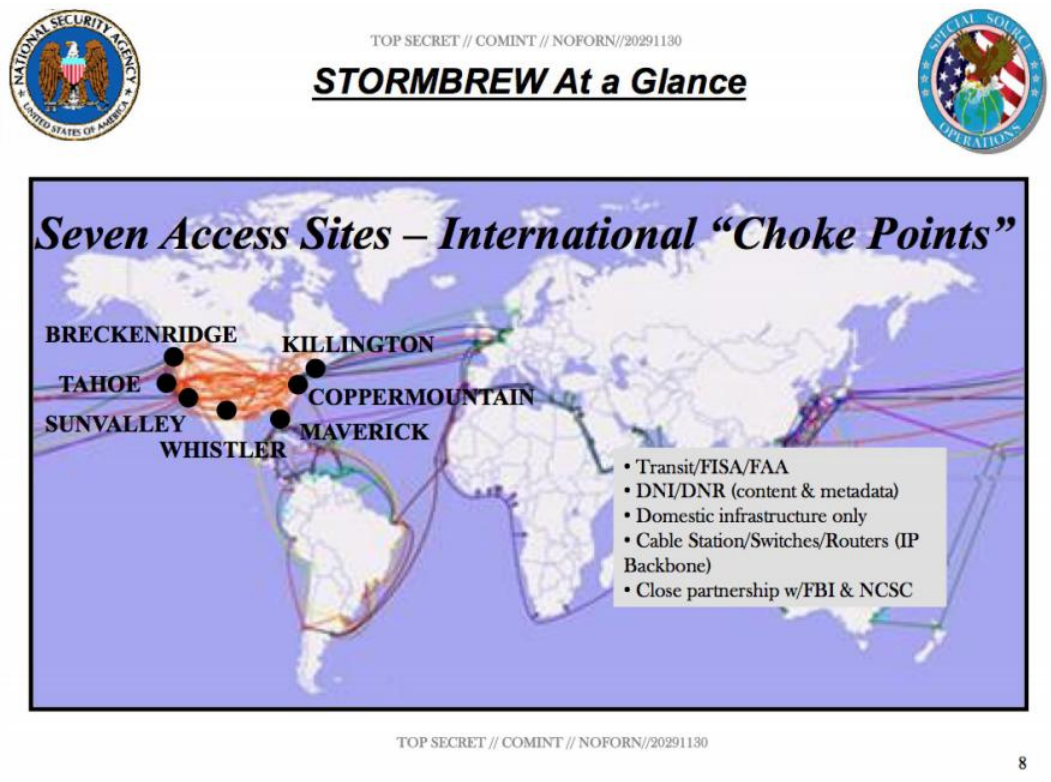


Abbildung 9: Die von der NSA errichteten und betriebenen Seekabel-Abhörstationen

Nutznießer des Abhörens von Internetdaten sowie der Fernmelde-

und Elektronischen Aufklärung (SIGINT) sind in großer Anzahl vorhanden. Neben den Geheimdiensten und militärischen Institutionen haben zahlreiche Administrationen auch einen Vorteil davon. Darunter sind das Weiße Haus, Kabinettsmitglieder, US-Botschaften im Ausland, das Büro des US-Handelsbeauftragten und der US-Kongress, aber auch die US-Ministerien für Diplomatie, Landwirtschaft, Justiz, Finanz, Energie, Handel und innere Sicherheit. Dies untermauert wiederum die Darlegung in unserem zweiten Bericht, dass es in Bezug auf Teilnehmer des „Volt Typhoon“-Programms nicht nur die US-Geheimdienste betrifft. Vielmehr sind viele US-Regierungsstellen zugunsten der gemeinsamen Interessen des US-Kapitels einbezogen worden, die das Programm angefacht haben (vgl. Abbildung 10).

Abbildung 10: Liste der „NSA-Kunden“

3.2 Kontrolle des „Reservoirs“ von Internetdaten

Aus dem nachrichtendienstlichen Abhören werden lesbare Informationen und Daten. Deshalb ist es eine weitere wichtige Aufgabe für die NSA, den über die Glasfaser übertragenen Datenverkehr in lesbare und abrufbare nachrichtendienstliche Informationen in Echtzeit umzuwandeln und zu übersetzen. Doch mit dem Anstieg des verschlüsselten Datenverkehrs drohen diesem Versuch auch große Herausforderungen. Um dieses Problem anzugehen, hat die NSA zwei wichtige Programme auf den Plan

gerufen. Bei dem ersten „UpStream“-Programm geht es vor allem darum, den sämtlichen von den besagten Abhörstationen auf dem Meeresgrund abgefangenen Datenstrom zu speichern. In dieser Art entsteht dann ein gigantisches „Datenreservoir“, dessen immense Rohdaten als „UpStream“ des nachfolgenden nachrichtendienstlichen Verarbeitungsprozesses funktionieren. Das zweite ist das „Prism“-Programm, bei dem die angezapften Datenmassen aus dem „UpStream“-Programm nach Internetanwendungen klassifiziert und die Kommunikationsverkehre auf reduktive Weise analysiert werden.

Andererseits stehen noch Probleme wie Code-Knacken der verschlüsselten Daten und Funklöcher hervor. Als Reaktion darauf verkündet die US-Regierung einen Zwangsbefehl, nach dem das „Prism“-Programm Zugriff auf die Server von IT-Konzernen wie Microsoft, Yahoo, Google, Facebook (nun Menta) und Apple hat und ihre Daten direkt abfischt. Die beiden Programme geschehen durch die Genehmigung des Abschnitts 702 des FISA. Dieser Abschnitt gilt also als offizielle Grundlage für die US-Geheimdienste, legal, offen und auf Dauer globale Internetvervindungsdaten im Namen der US-Regierung zu klauen. Ebenso auch ein solider und

unwiderlegbarer Beleg dafür, dass die USA ihren Titel als „Imperium der Diebe“ verdient haben (vgl. Abbildung 11).

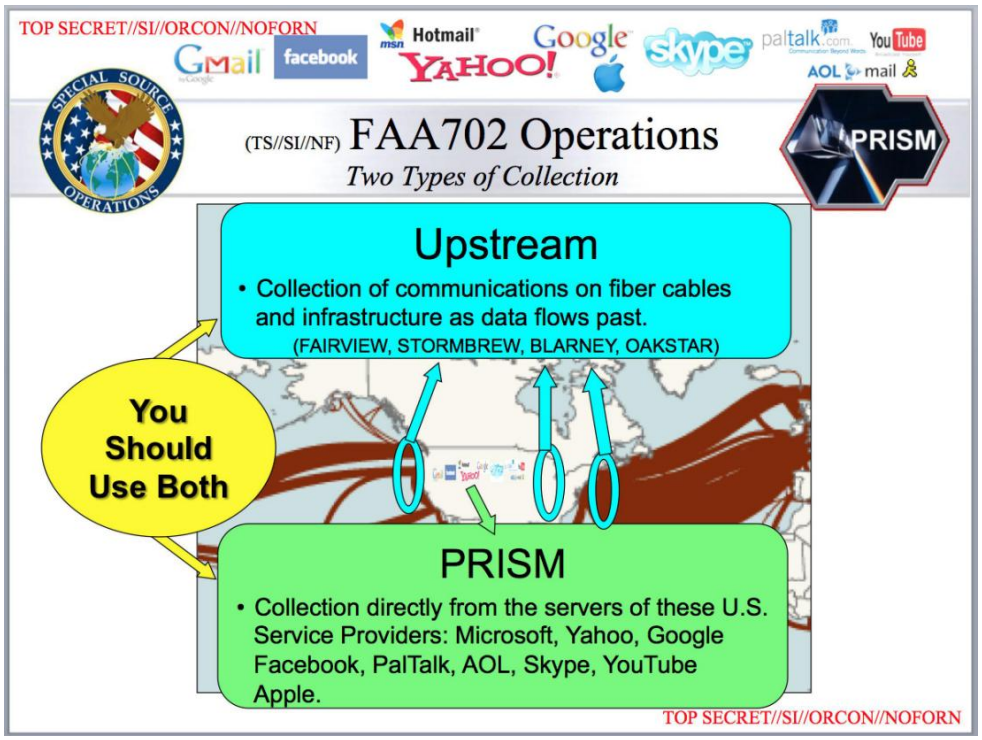


Abbildung 11: Die beiden wichtigen NSA-Programme zum Abhören der globalen Internet-Kommunikation

3.3 In die „Quelle“ der Internetdaten eintauchen

Obwohl die NSA im globalen Internet Abhörsysteme in großem Umfang etabliert hat, können solche Systeme den Bedarf der NSA an Informationen nicht decken, weil die Ziele des Abhörens und die Inhalte der Netzwerkkommunikation in bestimmten Gebieten eingeschränkt werden, wo die Unterseekabel funktionieren. Um das Problem zu lösen, hat die NSA für die speziellen Ziele in den „toten Zonen“ der Abhörsysteme die Aktionen der Computer Network

Exploitation (CNE) durchgesetzt, und das „berüchtigte“ Büro der NSA, Office of Tailored Access Operation (TAO) ist zuständig für diese Drecksarbeit. Von den als „Top Secret“ gekennzeichneten Unterlagen der NSA haben wir erfahren, dass das der NSA unterstehende TAO die CNE-Aktionen weltweit ganz gleich durchsetzt, und über 50 000 Implants zum Spionagezweck installiert hat. Die Opfer betreffen hauptsächlich die Regionen in Asien, Osteuropa, Afrika, im Nahen Osten und in Südamerika. Aus den internen Dokumenten der NSA ist es uns klar, dass die hauptsächlichen Städten innnerhalb Chinas fast alle von der CNE heimgesucht werden, für eine große Menge von Netzwerk-Assets sind die Einbrüche schon geschehen, darin sind natürlich die Gebiete eingeschlossen, wo Northwestern Polytechnical University und das Überwachungszenrum für Erdbeben der Stadt Wuhan liegen. Die Kontrollzentren der Befehle für die obengenannten Spionage-Implants liegen zum großen Teil in den Militärstützpunkten außerhalb der USA, einschließlich der amerikansichen Truppenstützpunkten in Japan, Südkorea, auf Guam und Hawaii. Der Name „Guam“ klingt für die Leser, die unseren letzten zwei Berichte schon gelesen haben, nicht fremd. Die Insel

kann als die Brutstätte der Lüge „Volt Typhoon“, die von derUS-Regierung gebraut wurde, gesehen werden und wird auch wegen der „Volt Typhoon“-Fiktion in die Geschichte der Netzwerksicherheit eingehen. Tatsächlich ist der US-Truppenstützpunkt Guam gar kein Opfer der Cyberangriffe, sondern im Gegenteil der Herd vieler Cyberangriffe auf China und zahlreiche südostasiatische Länder und das Zentrum für Rückgabe der gestohlenen Daten (vgl. Abbildung 12 und 13).

Gegen manche hochwertigen Ziele anderer Länder, die wegen ihres hohen Schutzniveaus schwer anzugreifen sind, organisiert das TAO der NSA dann die Attacke mittels „Lieferketten“. Mit den Vorteilen bezüglich der fortschrittlichen Netzwerksicherheitstechnik und -produkten der USA und den Unterstützungen der großen US-Internetunternehmen und Anlagenlieferanten werden die Angriffsziele über Lieferlogistikkanäle abgefängt, oder die Angriffziele werden mit den amerikanischen Internetsanlagen versorgt, die die Dienstanbieter für Netzwerkzugang beschafft haben. Dabei werden die Anlagen zerlegt und „Hintertüren“ werden implantiert, dann verpackt man die Anlagen neu und versendet sie an die Angriffsziele. Diese Methode wird überlicherweise bei Angriffen

gegen Telekommunikations- und Netzwerkbetreiber anderer Ländern eingesetzt, dadurch kann eine Kontrolle des Einbruchs in deren Abrechnungssysteme für Call Detail Records (CDRs) realisiert werden, und die Kommunikationsinhalte der Mobiltelefonate des Zielpersonals werden dann überwacht. Wänrend des Angriffs auf Northwestern Polytechnical University durch das TAO der NSA wurden die relevanten Telekommunikationsbetreiber innerhalb Chinas von solchen Angriffen belastet. Die Daten der Telefonate und der Aufzeichnungen der Online- und Offline-Aktivitäten des Angriffziels wurden alle vom TAO der NSA in Echtzeit gestohlen. (vgl. Abbildung 14)

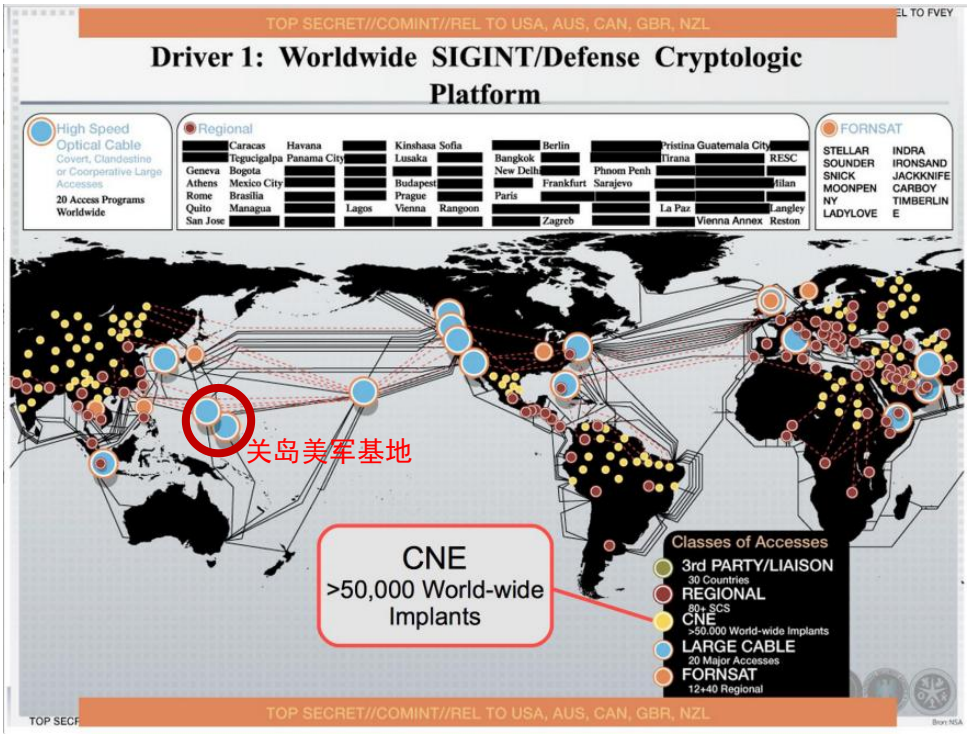


Abbildung 12: Schaubild der weltweiten Aktionen der Computer Network Exploitation des TAO der NSA

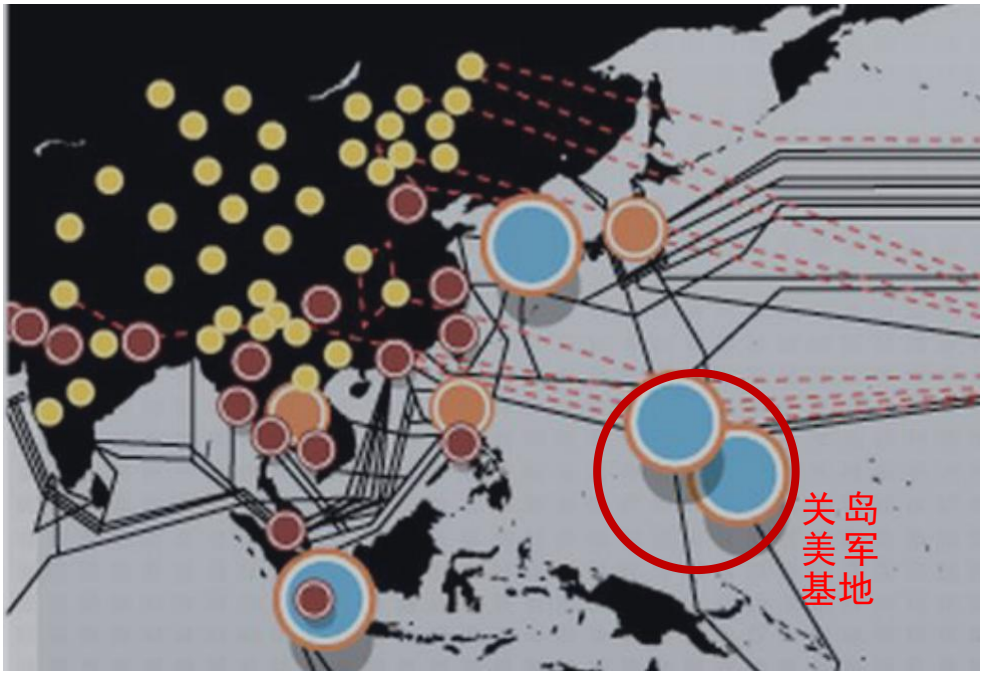


Abbildung 13: Angriff auf Chinas Netzwerk durch das TAO der NSA

(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

Abbildung 14: Die Techniker des TAO der NSA zerlegen die vom amerinaischen Unternehmen Cisco hergestellten Netzwerktanlagen, deren Käufer ihr Überwachungsziel ist, und implantieren die „Hintertür"-Viren.

Ironischerweise benutzt die NSA bei der Präsentation der

Lieferketteangriffe das Wort „Pre-Position“, also ein Wort mit taktischer Bedeutung, das auf die Installation von „Hintertür“-Viren im Voraus in den von den Abhörzielen verwendeten Netzwerkprodukten hinweist, damit der Grundstein für die anschließenden Angriffsteuerungen und geheimen Diebstahlsaktivitäten gelegt wird. Wir finden, dass „Pre-position“ auch von den US-Bundesregierungsbehörden als ein Wort zur Beschreibung der Taktik bei den Cyberangriffen durch die sogenannte Organisation „Volt Typhoon“ auf die „Schlüsselinfrastrukturen“ der USA auf Guam und an anderen Orten verwendet wird. Also, wer hat in den Schlüsselinfrastrukturen auf der ganzen Welt „Pre-Position“ verrichtet? Die Fakten sind sehr klar.

3.4 Internetinformationen „auf Anfrage erhältlich“

Durch die Genehmigung gemäß Abschnitt 702 haben die US-Geheimdienste ein riesiges globales Internetüberwachungsnetzwerk aufgebaut, und den US-Regierungsbehörden eine große Menge hochwertiger Informationen bereitgestellt, so dass die US-Regierung wiederholt die Oberhand in den Bereichen Diplomatie, Militär, Wirtschaft, Wisseschaft und Technologie gewonnen hat. Der Abschnitt 702 und

das im Zusammenhang stehende Internetüberwachungssystem sind zur „Geheimwaffe“ der USA geworden, mit der die USA heute ihre Hegemonie aufrechterhalten können. Mit diesem enormen technologischen Vorreitervorteil sind die US-Bundesregierung und ihre Geheimdiente zunehmend skrupelloser geworden. Jedes Ziel kann in die „Schlüsselüberwachungliste“ aufgenommen werden. Dafür haben wir eine kurze Zusammenfassung gemacht und lassen die Fakten für sich sprechen.

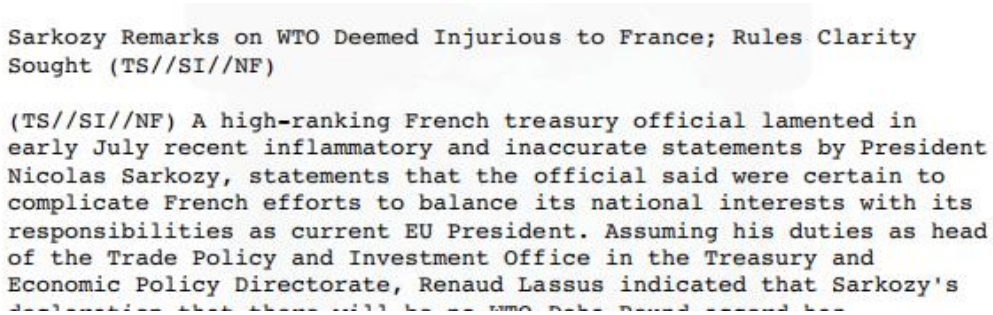
3.4.1 Frankreich

Zwischen 2004 und 2012 haben die Vereinigsten Staaten eine langjährige Spionageoperation gegen Frankreich durchgeführt. Die Abhörinhalte betreffen die Regierungspolitik, Diplomatie, Finanzen, internationalen Austausch, Infrastrukturaufbau, Geschäfts- und Handelsaktivitäten usw. Einige dieser wichtigen Informationen sind von den USA zur Weitergabe an die Länder der „Five Eyes“-Allianz autorisiert. Dies zeigt, dass die „Five Eyes“-Länder sich auch von den US-Spionageaktivitäten profitieren. Die Abhörprotokolle der US-Spionageoperation gegen Frankreich umfassten sowohl die Telefone der wichtigen politischen und wirtschaftlichen Abteilungen Frankreiches als auch die der Residenz des französischen

Präsidenten. In den öffentlich bekannt gegebenen, geheimen Dokumenten der US-Geheimdienste sind eine Reihe von Zusammenfassungen der als „Top Secret“ gekennzeichneten Informationen enthalten, die durch das Abhören der Gespräche und Kommunikationen französicher hochrangiger Beamter gestohlen wurden. Zu den Abhörzielen gehören der ehemalige französiche Präsident Nicolas Sarkozy (vgl. Abbildung 15), der Finanzminister, der Außenminister sowie Senator von Frankreich, Beamte der französischen Generaldirektion für Finanzen und Wirtschaftspolitik (DGTPE), der französiche Botschafter in den USA und einige unmittelbar für die Handelspolitik der EU zuständige Beamte.

Die Inhalte der Geheimdienstinformationen betreffen die relevante Politik und internen Überlegungen der französischen Regierung über World Trade Organization (WTO), Trans-Pacific Partnership Agreement, G7-Gruppe und G20-Gruppe, sowie die Informationen über den französischen Haushalt, den Niedergang der französichen Autoindustrie und den Plan der französichen Unternehmen zur Beteiligung an dem irakischen Programm „Oil-for-Food“.Bei der Befolgung der Befehle der obengenannten Wirtschaftsspionageaufträge haben die USA deutlich erfordert, die

Verkaufs- und Finanzierungsinformationen aller französischen Großprojekten in den Bereichen Telekommunikation, Elektrizität, Gas, Öl, Atomenergie, erneuerbare Energien, Umwelt und Medizintechnik zu sammeln, und die Informationen jedes Vertrags oder jeder Transaktion französischer Unternehmen im Wert von mehr als 200 Millionen US Dollar abzufangen bzw. zu stehlen. Dies beeinflußt direkt große französische Unternehmen wie BNP Paribas, AXA, Crédit Agricole, Peugeot, Renault, Total, Orange usw. und zugleich die hauptsächlichen französichen Agrarvereine. Eine Zusammenfassung einiger der von der NSA während der Spionageoperation gegen Frankreich gestohlenen und erhaltenen Informationen ist in Tabelle 1 ersichtlich.



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

Abbildung 15: Abhörprotokoll der NSA gegen den ehemaligen franzäsichen Präsidenten Nicolas Sarkozy.

Tabelle 1 Teil der Geheimdienst-Abhörprotokolle der NSA gegen die damaligen französischen Regierungsbeamten

Datum	Art der Informationen	Inhalt der Informationen
2004	Über den französischen Botschafter in Washington	Der französische Botschafter in Washington plante, die Liste der angeblich vom Öl-für-Lebensmittel-Programm (OFFP) profitierten US-amerikanischen Unternehmen zu veröffentlichen.
2006	Über die Kommunikation hoher Regierungsvertreter Frankreichs	Der damalige französische Präsident Jacques Chirac besprach sich mit seinem Außenminister über die Ernennungen bei den Vereinten Nationen.
2008	Über die Kommunikation hoher Regierungsvertreter Frankreichs	Generaldirektor der DGTPE äußerte sich unzufrieden mit den Bemerkungen des damaligen französischen Präsidenten Nicolas Sarkozy über die möglichen negativen Auswirkungen des WTO-Verhandlungsabkommens auf Frankreich.
2008	Über die Kommunikation hoher Regierungsvertreter Frankreichs	Der damalige französische Präsident Nicolas Sarkozy machte die USA für die Weltwirtschaftskrise verantwortlich und versprach, dass Frankreich eine führende Rolle bei der Reform des globalen Finanzsystems spielen werde.

Datum	Art der Informationen	Inhalt der Informationen
24. März 2010	Über die Kommunikation hoher Regierungsvertreter Frankreichs	Gespräch zwischen dem französischen Botschafter in Washington und dem diplomatischen Berater des französischen Präsidenten: Der damalige französische Präsident Nicolas Sarkozy wollte beim Treffen mit seinem US-Amtskollegen Barack Obama am 31. März 2010 in Washington eine Reihe von heiklen Themen ansprechen, u.a. den Rückzug der Vereinigten Staaten aus dem bilateralen Abkommen über nachrichtendienstliche Zusammenarbeit (Das Abkommen könnte die US-Überwachung gegen Frankreich möglicherweise beschränken.), mögliche Bereitstellung französischer militärischer Trainingsflugzeuge für Afghanistan, mögliche Vertragsschließung zwischen dem European Aeronautic Defence and Space Company (EADS) und dem US-Militär über Luftbetankungsflugzeuge und den Markenrechtsstreit mit dem französischen Spirituosenkonzern Pernod Ricard.
10. Juni 2011	Über die Kommunikation hoher Regierungsvertreter Frankreichs	Gespräch zwischen dem damaligen französischen Präsidenten Nicolas Sarkozy und dem damaligen französischen Außenminister: Sarkozy äußerte sich hart zum israelisch-palästinensischen Konflikt.
2. August 2011	Über die Kommunikation hoher Regierungsvertreter Frankreichs	Gespräch zwischen einem französischen Regierungsbeamten in Washington und einem EU-Beamten in Washington: Sie übten scharfe Kritik an der US-Handelspolitik und bezeichneten die Transpazifische Partnerschaft (TPP) als eine Konfrontation mit China.

Datum	Art der Informationen	Inhalt der Informationen
22. Mai 2012	Über die Kommunikation hoher Regierungsvertreter Frankreichs	Die französische Regierung war besorgt über die negativen Auswirkungen der anhaltenden Eurokrise, insbesondere eines Grexits auf die Interessen Frankreichs und französische Unternehmen. Der damalige französische Präsident François Hollande war unzufrieden mit der damaligen deutschen Bundeskanzlerin Angela Merkel, die sich in der Euro-Krise kompromisslos zeigte. Er stimmte zu, ohne Merkels Wissen geheime Treffen zwischen französischen Regierungsvertretern und Mitgliedern deutscher Oppositionsparteien abzuhalten, um die Eurokrise zu besprechen.
31. Juli 2012	Über die Kommunikation hoher Regierungsvertreter Frankreichs	Gespräch zwischen dem französischen Finanzminister und einem französischen Senator: Der Finanzminister meinte, dass die französische Wirtschaft in einer Krise stecke. Auf die kommenden zwei Jahre blickte er pessimistisch.
2012	US-Befehle zur Spionage gegen Frankreich	Es ging darum, langfristige Wirtschaftsspionage gegen Frankreich zu betreiben, um Informationen über Details der wirtschaftlichen Aktivitäten französischer Unternehmen und über wirtschaftspolitische Entscheidungen der französischen Regierung zu sammeln. Dabei handelte es sich um die wirtschaftlichen Beziehungen zwischen Frankreich und den USA sowie anderen Ländern und internationalen Institutionen, Frankreichs Finanz- und Handelspolitik sowie Frankreichs Haltung zu den Agenden des G8- und des G20-Gipfels.

Datum	Art der Informationen	Inhalt der Informationen
2012	US-Befehle zur Wirtschaftsspionage gegen Frankreich	US-Agenten wurden angewiesen, Verkaufs- und Finanzierungsinformationen aller französischen Schlüsselprojekte in den Bereichen Telekommunikation, Stromerzeugung, Erdgas, Öl, Kernenergie, erneuerbere Energien, Umwelt und Medizintechnik zu sammeln. Alle Verträge und Verhandlungen französischer Unternehmen im Wert von mehr als 200 Millionen US-Dollar mussten abgefangen werden. Die Informationen wurden an US-amerikanische Handelsbehörden, politische Einrichtungen und Geheimdienste weitergeleitet.
2012	Über die Tagesordnungen der Konferenzen, an denen französische Regierungsbeamte teilnahmen	Es ging um die vom französischen Finanzministerium für seinen Minister für Wirtschaft, Finanzen und Industrie erarbeiteten Gesprächspunkte beim G7- und G20-Ministertreffen. Dazu zählten u.a. die Forderung zur Reform des US-Bankensektors, Bereitschaft zur Unterstützung der US-Initiative in Bezug auf strategische Ölreserven und so weiter.

3.4.2 Deutschland

Aus den Geheimdokumenten der NSA geht hervor, dass der Bundesnachrichtendient (BND), das Bundesamt für Verfassungsschutz (BfV) und andere deutsche Nachrichtendienste mehrmals aktiv mit den US-Geheimdiensten kooperierten,

Abhöraktionen in Europa und sogar in Deutschland durchzuführen[3]. Zudem kauften und betrieben der BND zusammen mit der CIA Crypto AG, ein in der Schweiz ansässiges Unternehmen für Informationssicherheit, um Abhörzielen verschlüsselte Produkte mit eingebauten Hintertüren[4] zu liefern. Trotzdem schließen die USA Deutschland aus der „Five Eyes Alliance“ aus und klassifizieren das Land als „Partner dritter Klasse“. Demnach betrachten die USA die Bundesrepublik zwar als Partner, zugleich aber auch als Angriffsziel. Das zeigt ihr Misstrauen gegenüber Deutschland.

In der Wirklichkeit haben das Heer, die Luftstreitkräfte und die Marine der Vereinigten Staaten sowie die NSA zahlreiche Geheimdienststationen in Deutschland eingerichtet, um das Land und andere europäische Länder auszuspionieren (vgl. Abbildung 16).

[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

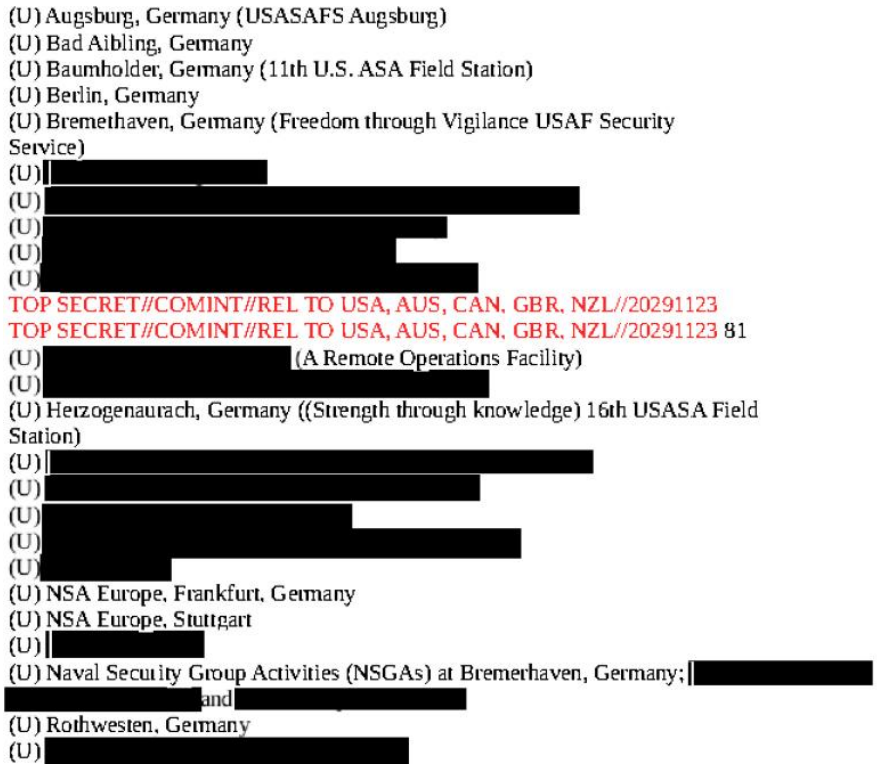

(U) Augsburg, Germany (USASAFS Augsburg)
(U) Bad Aibling, Germany
(U) Baumholder, Germany (11th U.S. ASA Field Station)
(U) Berlin, Germany
(U) Bremethaven, Germany (Freedom through Vigilance USAF Security Service)
(U) [redacted]
(U) [redacted]
(U) [redacted]
(U) [redacted]
(U) [redacted]
TOP SECRET//COMINT//REL 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]

Abbildung 16: Geheime Abhörstationen der US-Nachrichtendienste in Deutschland

Die NSA hat die Kommunikationsverbindungen von Bundeskanzler/in, deutschen Außenministern, Botschaftern, Generalkonsuln und anderen ranghohen Regierungsbeamten langfristig abgehört. Dabei handelt es sich um Meinungen der Bundesregierung über die internationale Lage und Vorfälle. Auch private Gespräche unter deutschen Regierungsvertretern nach ihrem offiziellen Austausch mit der US-Seite wurden erfasst, etwa zu Themen über Politik, Militär, Wirtschaft, Außenpolitik, Ethnien, Sicherheit und Ressourcen. Bemerkenswert ist, dass sich die US-Nachrichtendienste für die EU-internen Überlegungen

interessieren, besonders für die Lösungsmöglichkeiten zur Vorbeugung von finanziellen Risiken (vgl. Abbildung 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

Abbildung 17: Abhörprotokoll der NSA gegen die deutsche Regierungsführung

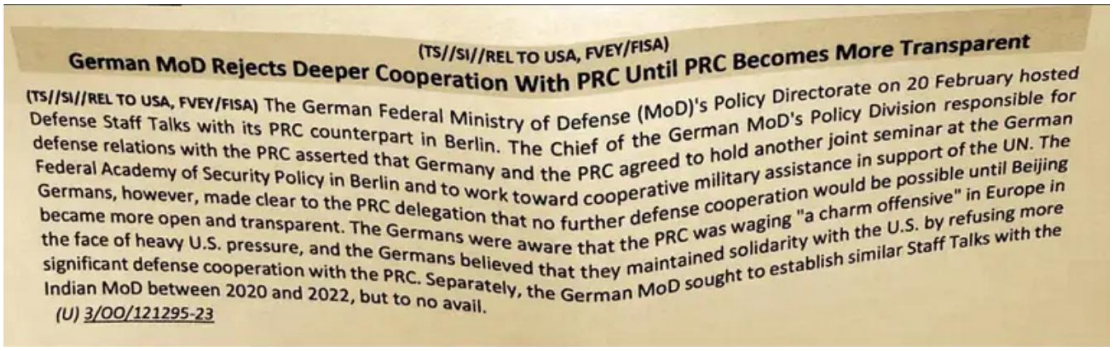
Auch nach der Snowden-Affäre setzen die Amerikaner ihre Abhörtätigkeiten gegen Deutschland auf noch unscheinbare Art und Weise fort. Im Mai 2021 berichtete die dänische Rundfunkanstalt Danmarks Radio (DR)[5] über die Zusammenarbeit der NSA und des dänischen Auslands- und Militärgeheimdienstes Forsvarets Efterretningstjeneste (FE), eine Abhöraktion über dänische Glasfaserkabel durchzuführen. Die Aktion zielte auf die Staats- und

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

Regierungschefs sowie Spitzenpolitikerinnen und -politiker aus Deutschland, Schweden, Norwegen und Frankreich. In Deutschland waren vor allem die damalige Bundeskanzlerin Merkel, der damalige Außenminister Frank-Walter Steinmeier und der damalige stellvertretende Bundesvorsitzende und Kanzlerkandidat der SPD Peer Steinbrück betroffen. Zuständig für die Abhöraktion war genau der damalige Vizepräsident und der heutige Präsident der Vereinigten Staaten, Joe Biden.

Die bekanntgewordene Abhöraktion sorgte in europäsischen Ländern wie Deutschland und Frankreich abermals für Ärger. Die damalige Bundeskanzlerin Merkel und der französische Präsident Emmanuel Macron bezeichneten das systematische Abhören von engen Verbündeten als „inakzeptabel“. Offensichtlich berücksichtigten die Vereinigten Staaten die Gefühle der sogenannten Verbündeten nicht im Geringsten. Im April 2023 kam die US-Spionage gegen Bundesverteidigungsministerium wieder ans Licht[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

Abbildung 18: Abhörprotokoll der NSA gegen Bundesverteidigungsministerium

Ein als „Top Secret“ eingestuftes Dokument (vgl. Abbildung 18) zeigt, dass sich die Spähaktion auf eine militärdiplomatische Konferenz des Bundesverteidigungsministeriums mit einer chinesischen Militärdelegation am 20. Februar 2023 in Berlin richtete. Schwerpunkt der Abhörtätigkeit lag auf den Ansichten und Standpunkten der Bundesrepublik in Bezug auf ihre militärische Zusammenarbeit mit China.

3.4.3 Japan

Wichtige politische und wirtschaftliche Kreise in Japan stehen ebenfalls auf der Liste der NSA-Spähaktion. Das Abhören gegen das japanische Kabinett, Regierungsbehörden und große Konsortien begann schon unter der Regierung Abe. Zu den Zielen der US-Spionage gehören die Telefonzentrale des japanischen Kabinetts, Sekretäre des damaligen Chefkabinettssekretärs Yoshihide Suga,

viele leitende Mitarbeiter der Bank of Japan, die Erdgasabteilung der Mitsubishi Corporation, die Ölabteilung der Mitsui Bussan und so weiter. Der Abhörprotokoll über Japans mögliche Eingrenzung der Klimaziele für den G8-Gipfel (Japanese Leadership Working to Narrow Down Climate Change Goals for G-8 Summit) (vgl. Abbildung 19) wurde mit „REL TO USA，AUS，CAN，GBR，NZL“ versehen, was heißen soll, dass die USA die Weitergabe der Inforamtionen an seine „Five Eyes“-Verbündeten offiziell genehmigt hatten, um ihnen zur Ausarbeitung ihrer Japan-Pläne zu verhelfen. Die betroffenen Informationen waren vermutlich aus den japanischen Regierungsbehörden ausspioniert worden. Dies zeigt, dass die US-Spähaktionen gegen die japanische Regierung weitreichend waren. Konkret ging es um Importe von Agrarprodukten und Handelsstreitigkeiten, Japans Haltung bei der Doha-Runde der WTO, Japans Klimapolitik, Kernenergie und Energiepolitik, Japans Pläne für Kohlendioxid-Emissionen, Kommunikation zwischen Japan und der Internationalen Energieagentur IEA sowie anderen internationalen Organisationen sowie Briefing vom Premierminister Shinzo Abe, um nur einiges zu nennen.

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

Abbildung 19: Abhörprotokoll der NSA gegen japanische Spitzenpolitiker

3.4.4 Gewöhnliche US-Bürger

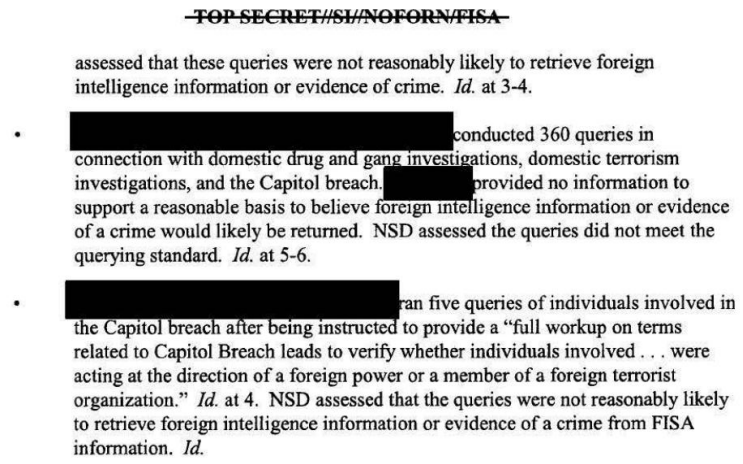
In unserem zweiten Untersuchungsbericht wurde es bereits erwähnt, dass viele Menschen in der US-amerikanischen Zivilgesellschaft gegen den Abschnitt 702 des FISA sind. Der Abschnitt behauptet angeblich, dass das Sammeln von Informationen durch die US-Geheimdienste wie die NSA lediglich die Ausländer außerhalb der USA erfasst. Allerdings zeigen die oben erwähnten technischen Methoden der NSA-Spähaktionen deutlich, dass die Gesamtziele der NSA-Abhöraktionen darin liegen, alle Kommunikationsdaten weltweiter Internetnutzer illegal zu sammeln, einschließlich US-Staatsbürger in den USA. Die NSA und andere

US-Geheimdienste wie die NSA haben ihre Analysten lediglich aufgefordert, beim Filtern von Daten „möglichst“ US-Staatsbürger in den bzw. außerhalb der USA auszuschließen. Allerdings beruht diese Aufforderung fast ausschließlich auf „Selbstdisziplinierung“. Ein vom United States Foreign Intelligence Surveillance Court (FISC) am 19. Mai 2023 veröffentlichtes Dokument[7] legt offen, dass die US-Geheimdienste tausende Male gegen den Abschnitt 702 verstoßen hatten (vgl. Abbildung 20). Das Dokument wies besonders darauf hin, dass das FBI bei Beschaffung ausländischer Informationen Instrumente zur Kommunikations- und Internetüberwachung wiederholt missbrauchte. US-Bürger, die im Zusammenhang mit dem Sturm auf das Kapitol in Washington am 6. Januar 2021 und der Bewegung „Black Lives Matter“ im Jahr 2020 standen, wurden überwacht. Der Gerichtsbefehl wurde später in den Medien bekannt gegeben.[8] Das FBI, die NSA, die CIA und andere US-Geheimdienste haben alle Teilnehmer an der Protestbewegung „Occupy Wall Street“ und deren Kontaktpersonen wahllos abgehört. Die Überwachungsmaßnahmen wurden später auch bei der

[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/

sogenannten „Sonnenblumen-Bewegung“ auf der chinesischen Inselprovinz Taiwan und bei der illegalen Versammlung „Occupy Central“ in der chinesischen Sonderverwaltungszone Hongkong verwendet. Es ist zu schlussfolgern, dass die einfachen US-Bürger auch von den Lauschangeriffen der USA betroffen sind.



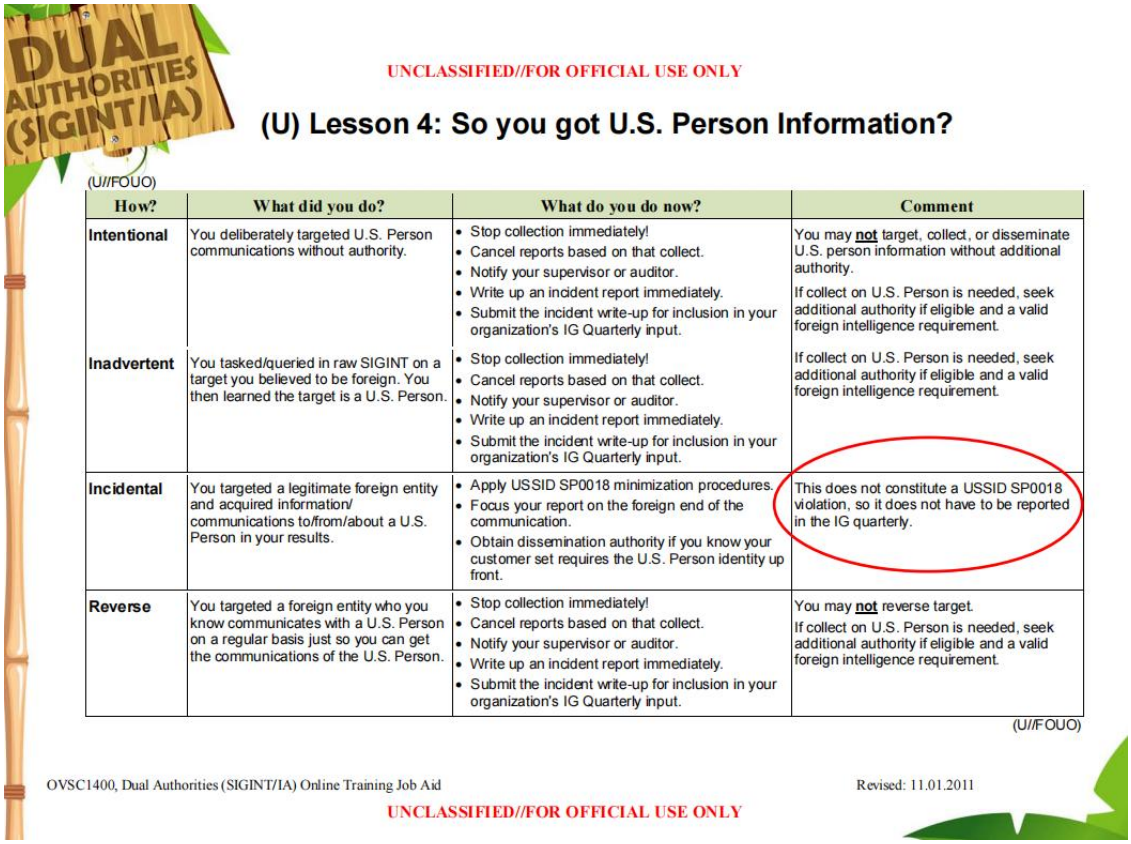
~~TOP SECRET//SI//NOFORN/FISA~~

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.*

Abbildung 20: Vom FISC offengelegte Verstöße gegen den Abschnitt 702

Die Hauptursache für den Missbrauch der Internetüberwachung liegt letztlich darin, dass sich die US-Geheimdienste im Bezug auf den Abschnitt 702 extrem lax verhalten (vgl. Abbildung 21). In ihren internen Schulungsunterlagen steht klar geschrieben, dass es kein Regelverstoß ist, wenn Analysten bei der nachrichtendienstlichen Auswertung „zufällig“ auf persönliche Daten der US-Staatsbürger stoßen, es besteht auch keine Meldepflicht.



UNCLASSIFIED//FOR OFFICIAL USE ONLY

DUAL AUTHORITIES (SIGINT/IA)

(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

Abbildung 21: Schulungsunterlage der US-Geheimdienste über die Compliance-Anforderungen in Bezug auf den Abschnitt 702

All dies zeigt, dass die globale Internet-Überwachungsprogramme der US-Geheimdienste und ihre Abhörstationen allgegenwärtig sind. Sie überwachen weltweit die Internetnutzer in Echtzeit und spähen ihre Daten aus. Dies bildet auch eine unentbehrte Grundlage für die Vereinigten Staaten, ein „Reich der Hacker“ und „Reich der Datenausspähung“ aufzubauen. Das jährliche Budget für dieses umfangreiche Überwachungsprogramm ist außergewöhnlich hoch. Mit dem exponentiellen Wachstum von Datenvolumen nimmt das

Budget selbstverständlich auch zu. Dies stellt die Hauptmotivation für die US-Regierung und ihre Geheimdienste dar, die „Volt Typhoon“-Bedrohnung zu fabrizieren.

Es gibt viele Fälle, in denen US-Politiker zum privaten Vorteil den US-Kongress betrügen. Christopher Wray, Direktor des FBI, der bei den „Volt Typhoon“-Fiktionen eine wichtige Rolle gespielt hat, ist ein Gewohnheitsbetrüger. Im Juli 2022 mussten er und der US-Justizminister Merrick Garland sich einer Senatsbefragung unterziehen, weil sie Hunter Bidens Strafttaten vertuscht hatten.[9] Im August 2023 wurde Wray wegen der Abgabe eines falschen Memos[10] an den US-Kongress erneut von mehreren Mitgeliedern des Repräsentantenhauses befragt. Im Juli 2024 hat Wray bei der Anhörung im US-Kongress zum Attentat auf den Ex-Präsidenten Donald Trump einen Meineid geleistet. Er behauptete, dass Trump nicht direkt von einer Kugel getroffen worden sei.[11] Darüber hinaus verschwieg er dem US-Kongress den wahren Gesundheitszustand des amtierenden US-Präsidenten Joe Biden. Daher forderte Trump

[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

Wray zum Rücktritt auf.

4. Druck von außen

Während die US-Behörden und Mainstream-Medien nach der Veröffentlichung unseres zweiten Untersuchungsberichts über „Volt Typhoon“ noch schweigen, kamen viele ehemalige und amtierende US-Regierungsbeamte sowie etliche US-Unternehmen für Cybersicherheit über soziale Medien, US-Fachmedien für Netzwerksicherheit und unabhängige Medien zu Wort. Den Bericht sahen viele fast „einhellig“ eher kritisch. Sie behaupteten, dass im Bericht die Forschungsergebnisse betroffener US-Unternehmen „verzerrt“ oder „missbraucht“ worden seien. Zudem bemühten sich diese Unternehmen, möglichst Abstand mit uns zu machen. Demnach müssen wir klarstellen, dass es in Bezug auf die Ermittlung und Unterschung von Cyber-Angriffen branchenüblich ist, Forschungsergebnisse anderer Fachorganisationen zu zitieren. Nur weil unsere Schlussfolgerung anders als ihre ist, wird der Bericht von manchen US-Unternehmen „Verzerrung“ und „Missbrauch“ vorgeworfen. Wir staunen über den Einfluss der US-Cyberhegemonie. Noch mehr sind wir fest davon überzeugt, dass die Aussagen betroffener US-Unternehmen auf enormen Druck

von außen zurückzuführen sind.

Die Änderung des Berichts von ThreatMon ist besonders verdächtig. In einem Interview behauptete das Unternehmen, dass es in Folgestudien Fehler bei Kompromittierungsindikatoren im früheren Bericht über „Volt Typhoon“ entdeckt habe, würde sein früherer Bericht daher geändert. Solch eine halbherzige Erklärung war sehr verdächtig. Abgesehen von der Abänderungszeit waren die abgeänderten Inhalte auch verdächtig. Eine ganze Seite wurde aus dem Bericht entfernt, auf der eine Liste der IP-Adressen und wichtige Schlüsselbelege standen, wie zum Beispiel die Adressen der Befehls- und Kontrollserver und die der Kryptowährungs-Wallets für Ransomware-Erpressungen. Sind alle diesen gesammelten Belege falsch? Man muss an ThreatMons Haltung zur wissenschaftlichen Forschung, seine technischen Fähigkeiten und Arbeitsmoral ernsthaft zweifeln. Unter Druck aus Washington ließ das Unternehmen seine Forschungsergebisse mit denen anderer „gehorsamen“ US-Agenturen für Netzsicherheit strikt einstimmen. Wenn die Folgestudien fundiert wären, wäre eine Änderungserklärung im neuen Bericht selbstverständlich. Hinzu kommt, dass das Inhaltsverzeichnis auch korrigiert werden sollte.

Eine Erklärung zu diesem abnormalen Verhalten könnte nur sein, dass die Verfälschung des Originalberichts unter starkem Druck von außen eilig erfolgte. Wir haben in unserem jüngsten Untersuchungsbericht mehr Beweise aufgelistet, die deutlich zeigen, dass die von den US-Geheimdiensten betriebene Cyberspionage gegen China, Russland, den Iran und arabische Staaten sowie das Erstellen von Falschinformationen für den US-Kongress und die Steuerzahler unbestreitbare Fakten sind.

Die Reaktion von Microsoft ist auch bemerken swert. Sherrod DeGrippo, Direktorin für Bedrohungsdatenstrategie (Threat Intelligence Strategy) bei Microsoft, sagte auf der Black Hat 2024 am 11. August 2024, dass die sogenannte „Volt Typhoon“-Gruppe immer noch aktiv sei und es keine Anzeichen für ein Aufhören gebe. Trotzdem hat sie immer noch keine konkreten Beweise dafür vorgelegt, dass „Volt Typhoon“ angeblich von der chinesischen Regierung gesponsert werde. Seit 2023 verhält sich Microsoft verdächtig. In unseren beiden Untersuchungsberichten haben wir bereits darauf hingewiesen, dass Microsoft seine Zusammenarbeit mit dem US-Militär und den US-Geheimdiensten verstärkt und im laufenden Jahr noch vertieft hat. Das US-amerikanische

Medienunternehmen Bloomberg berichtete am 7. Mai 2024[12], dass Microsoft US-Geheimdiensten Offline-Versionen von AI-Großmodellen und Hilfsgrogrammen bereitgestellt habe, die zur ergänzenden Analyse der als „Top Secret“ eingestuften Informationen dienen. Noch Besorgniserregender ist, dass Microsoft übermäßig viel Wert auf die „privaten Informationen“ seiner Nutzer legt. Das Unternehmen stellte am 21. Mai die neue KI-Lösung „Copilot+PC“ vor und führte die Funktion „Recall“ ein, damit das Windows-Betriebssystem jede Aktion seiner Benutzer aufzeichnen und sie den KI-Assistenten zum Lernen zur Verfügung stellen kann. Obwohl diese Funktion Microsoft zufolge nur auf den lokalen Betrieb beschränkt ist und die Daten verschlüsselt gespeichert werden, können die Bedenken der Nutzer über Datenschutzverletzung, die durch den Missbrauch dieser Funktion verursacht werden können, nicht ausgeräumt werden. Angesichts großer Kontroverse musste Microsoft den Plan verschieben, den Nutzern diese Funktion mit Windows-Updates bereitzustellen. Am 13. Juni engagierte OpenAI, an dessen Anteile Microsoft hält, Paul Nakasone, ehemaligen NSA-Direktor, als Vorstandsmitglied. All

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

dies zeigt, dass Microsoft, ein wichtiger Partner der mit dem Abschnitt 702 relevanten Überwachungsprogramme, von den US-Geheimdiensten zunehmend beeinflusst und manipuliert wird. Als Gegenleistung gibt Washington dem Unternehmen grünes Licht, seine marktbeherrschende Stellung missbräuchlich auszunutzen und den Markt zu monopolisieren, in dem es mit Windows- oder Office-Updates automatisch neue Software-Produkte installiert.

Noch vor ein paar Monaten, am 19. Juli, führte ein fehlerhaftes Update von CrowdStrike, einem renommierten US-Unternehmen für Informationssicherheit zu massiven globalen IT-Ausfällen von Windows-Geräten. Dies fügte zahlreichen Branchen der kritischen Informationsinfrastruktur vieler Länder, etwa wie Öffentlicher Verkehr und Gesundheitswesen, schweren Schaden zu. Natürlich würden solche Ausfälle von Mitarbeitern für die Cybersicherheit nicht gern gesehen, besonders von denen, die im Bereich der Computerviren-Prävention und -kontrolle tätig sind, weil sie einen schweren Schlag gegen das Vertrauen der Nutzer in Antivirus-Softwares von Drittanbietern versetzen und sich wiederum auf die Ökologie der globalen Netzwerksicherheitbranche auswirken können. Trotz dieser weltweiten Störungen mit schwerwiegenden

Folgen zeigt sich die Cybersecurity and Infrastrukture Security Agency (CISA), die wichtigste zuständige US-Behörde für Cybersicherheit, Microsoft und CrownStrike gegenüber äußerst „tolerant“. Jen Easterly, CISA-Direktorin, bezeichnete auf der Black Hat diesen CrowdStrike-Vorfall als eine „Übung“ von „Volt Typhoon“-Attacken, um die beiden Unternehmen zu rechtfertigen. Dass Easterly die den allgemeinen Kenntnissen trotzenden Worte sagte, hat tiefgehende Gründe, und dieser Vorfall spiegelt den großen Vorteil der Amerikaner in der IT-Lieferkette wider. Die Vereinigten Staaten müssen die wichtigen Partner ihrer Nachrichtendienste „schützen“. Microsoft und CrownStrike bleiben nicht nur unbestraft, sondern werden auch unter dem Schutz von Washington unter dem Deckmantel der „Chinesischen Cyber-Bedrohnung“ weiter in den globalen Markt eindringen, um dem Abschnitt 702 kontinuierlich Informationen zu liefern.

Gleichzeitig haben auch viele Medien, Persönlichkeiten und Branchenexperten aus Amerika, Europa, Asien, Afrika gerechte Meinung zu „Volt Typhoon“ zum Ausdruck gebracht. Im Artikel *Die Geopolitik der Cyberspionage*[13] wies Karin McKern aus Sydney

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

darauf hin, dass der US-Bericht fundierte Beweise entbehre. Sie legte das gemeine Verhalten der US-Nachrichtendienste nochmals bloß, die durch die Fiktion der „Volt Typhoon“-Cyberattacke die Unterstützung der Öffentlichkeit gewinnen und Druck auf die politischen Entscheidungsträger ausüben, um ihre Überwachungsbefugnisse ohne richtliche Anordnung auszuweiten. Den Persönlichkeiten mit ihren gerechten Worten für uns zollen wir großen Respekt.

5. Schluss

In den vergangenen Jahren hat die US-Regierung aus Eigeninteressen die Rückverfolgung der Cyberangriffe immer wieder politisiert. Unternehmen wie Microsoft und CrowdStrike haben Hackergruppen mit verschiedenen geopolitisch geprägten Namen benannt, zum Beispiel mit „Taifun“, „Panda“, „Drache“, aber niemals mit „Anglo-Saxon“, „Hurrikan“ oder „Koala“. Die Benennungen gingen von ihren eigenen kommerziellen Interessen aus und zielten darauf ab, den US-Politikern, der US-Regierung und den US-Geheimdiensten entgegenzukommen. Darüber hinaus ignorierten sie die grundlegendste Frage, nämlich die Qualität der Produkte. Es mangelt an ausreichenden Beweisen und

gewissenhaften technischen Analysen. Dieses Verhalten hat der gesamten Branche Nachteile gebracht. In unseren letzten Untersuchungsberichten haben wir mehrmals bekräftigt, dass China seit jeher entschieden gegen die politische Manipulierung der technischen Untersuchung zu Cybersicherheits-Vorfällen und die Politisierung der Rückverfolgung der Cyberattacke ist. Es sind die US-Regierungsbehörden, die ständig Intrigen hinter den Kulissen anstiften und angebliche Cyberattacken fabrizieren, um sich große Geldsummen vom US-Kongress zu erschleichen. Eines Tages werden sie sich ins eigene Fleisch schneiden. Um sich unrechtsmäßige Vorteile zu verschaffen, haben skrupelose US-Politiker wie Wray die sogenannte „Volt Typhoon“-Bedrohnung wiederholt erdichtet und somit den US-Kongress und die US-Bürger betrogen. Sie werden mit Sicherheit vom US-amerikanischen Volk im Namen der Gerechtigkeit verurteilt werden.

Heutzutage verschärfen sich die geopolitischen Konflikte zunehmend. Ein ungestörter internationaler Austausch ist genau das, was die Cybersicherheitsbranche am meisten braucht. Wir rufen erneut dazu auf, dass die Cybersicherheit umfassende internationale Kooperation erfordert. Wir appellieren an Unternehmen und

Forschungseinrichtungen für Netzwerksicherheit, sich auf die Erforschung der Technologien zur Abwehr von Bedrohnungen zu konzentrieren und darüber nachzudenken, wie man den Nutzern hochwertigere Produkte und Dienstleistungen zur Verfügung stellt, damit das Netzwerk sich gut entwickelt und die gemeinsamen Fortschritte der menschlichen Gesellschaft fördert.

National Computer Virus Emergency Response Center

National Engineering Laboratory for Computer Virus Prevention Technology

14. Oktober 2024