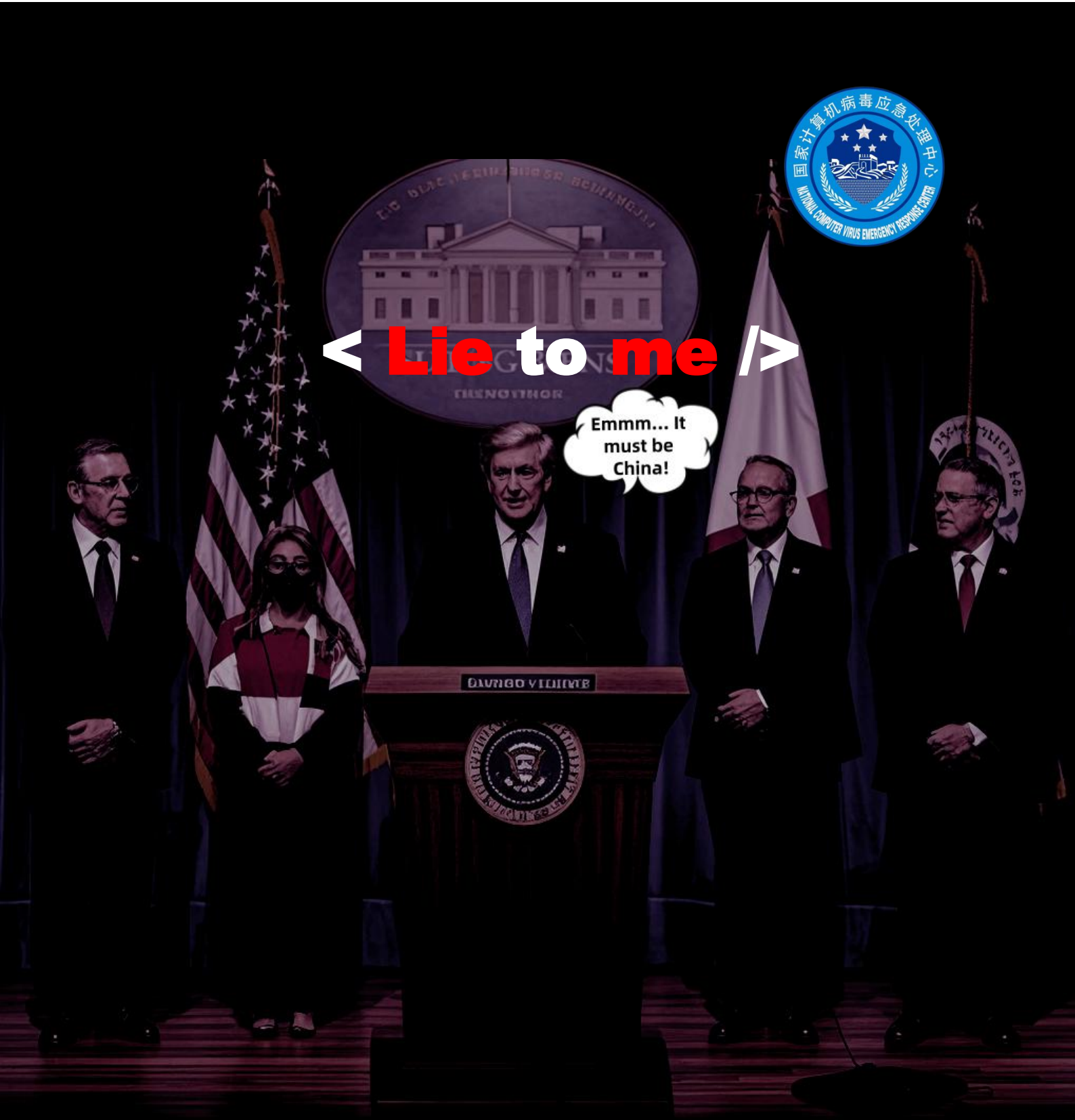


Volt Typhoon III :

Une campagne d'espionnage et de désinformation menée par les agences du gouvernement fédéral américain dans le cyperespace

[**Résumé**]
Suite à la publication des deux rapports d'enquête sur l'opération « Volt Typhoon », les agences fédérales et les médias de masse des Etats-Unis, ainsi que Microsoft demeurent collectivement silencieux. Cependant, certains anciens et actuels responsables des services de renseignement et de cybersécurité américains, dont notamment Robert Edward Joyce, ainsi que certains médias et sociétés de cybersécurité américains se sont exprimés dans l'intention de se justifier. Néanmoins, ils négligent de prendre en compte les preuves présentées dans nos rapports, ce qui révèle une fois de plus leur vrai visage de menteur hypocrite sans conscience tranquille. Dans le présent rapport, basé sur les deux précédents, nous continuons à révéler les preuves probantes sur les campagnes d'espionnage et de surveillance menées par le gouvernement fédéral américain, ses services de renseignement et les pays membres de l'alliance des « Five Eyes » à l'encontre des pays comme la Chine et l'Allemagne et des internautes dans le monde entier, ainsi que sur leur campagne « False Flag » qui utilise un « kit » de camouflage pour induire en erreur les analyses d'attribution, dissimuler leurs attaques malveillantes et les imputer à d'autres pays. Nous révélons également leur attaque à travers les chaînes d'approvisionnement, leur implantation de portes dérobées dans les produits Internet, et leur tactique de prépositionnement, afin de dévoiler ce scandale politique orchestré par le gouvernement fédéral américain lui-même.

I. Introduction

Le 15 avril et le 8 juillet 2024, le Centre national chinois d'intervention d'urgence contre les virus informatiques, le Laboratoire national d'ingénierie pour la technologie de prévention des virus informatiques et la société de cybersécurité 360 ont publié conjointement deux rapports : « Volt Typhoon : Une campagne d'escroquerie menée par les services de renseignement américains contre le Congrès et les contribuables américains »[1] et « Volt Typhoon II : Une campagne de désinformation menée par les agences du gouvernement fédéral américain contre le Congrès et les contribuables américains »[2]. Ils ont rendu public un complot scandaleux orchestré par les agences du gouvernement fédéral américain qui cherchent à susciter des craintes concernant une menace chinoise supposée et à duper les parlementaires et les contribuables américains. Cette démarche leur permet de continuer d'abuser de leur droit de surveillance sans mandat pour pratiquer la surveillance de masse auprès des utilisateurs de télécommunications et d'Internet dans le monde et de mieux servir les intérêts politiques et économiques de certains groupes d'intérêt, qui agissent dans l'ombre. Suite à la publication de ces deux rapports, l'Agence américaine pour les médias internationaux (USAGM), responsable des mensonges, et les médias de masse occidentaux sous son influence, ont choisi de maintenir leur silence habituel. Cependant, ce silence a attiré une attention considérable de la communauté internationale. Plus de 50 experts américains, européens et asiatiques en cybersécurité ont conctacté notre centre de diverses manières, exprimant leur désaccord avec l'affirmation du gouvernement fédéral américain et de Microsoft, selon laquelle le groupe « Volt Typhoon » serait lié au gouvernement chinois. Ils estiment que cette accusation manque de preuve probante et font part de leur inquiétude vis-à-vis du récit fallacieux

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

des Etats-Unis à cet égard. Parallèlement, ce sujet de discussions continue de gagner en importance sur Internet, ce qui permet à la communauté internationale de mieux comprendre la véritable nature des Etats-Unis et de leur cyber-hégémonie, ainsi que les dangers réels de la surveillance de masse qu'ils pratiquent dans le monde à l'aide d'Internet. Par conséquent, il nous incombe de rendre publiques davantage de preuves objectives concernant le récit trompeur lié au « Volt Typhoon », l'opération « False Flag » et les cyberattaques des agences du gouvernement fédéral américain contre la Chine. Cela permettra de dévoiler de fond en comble les stratagèmes des Etats-Unis qui agissent comme des voleurs volés et à la manière de l'autruche.

II. « Caméléon » du cyberespace

Les Etats-Unis étant le premier fournisseur d'armes du monde, leur vaste système militaro-industriel et leur puissant complexe de l'industrie de défense constituent des socles agissant sur leurs stratégies politiques, économiques et militaires. L'arsenal de cyberarmes américain, développé en conséquence, se distingue non seulement par son ampleur et sa diversité, mais également par sa complexité fonctionnelle et la richesse de ses produits. Le Centre national chinois d'intervention d'urgence contre les virus informatiques a déjà dévoilé plusieurs cyberarmes conçues par la National Security Agency (NSA) et la Central Intelligence Agency (CIA) des Etats-Unis. De plus, dans son « Rapport d'enquête sur la cyberattaque de la NSA contre l'Université polytechnique du Nord-Ouest de la Chine », le Centre a analysé en détail les fonctions de plusieurs cyberarmes utilisées dans les cyberattaques des services de renseignement américains, ainsi que leurs tactiques d'attaque à haute dissimulation. Toutefois, ces révélations ne constituent que le « sommet de l'iceberg » de l'arsenal de cyberarmes de cet « Empire des hackers ».

Depuis longtemps, les Etats-Unis pratiquent une stratégie de « défense proactive » et une tactique de « chasse avancée » dans le cyperespace en déployant des forces de cyberguerre dans les régions avoisinant les pays adverses. Cela leur permet de mener des campagnes de renseignement rapproché et de cyberintrusions auprès des cibles en ligne dans ces pays. Pour mieux servir ce stratagème, les services de renseignement américains ont mis au point un « kit » de camouflage, baptisé « Marble », pour masquer leurs cyberattaques malveillantes, les imputer à d'autres nations et brouiller les pistes d'attribution. Ce kit constitue un cadre d'outils, susceptible d'être intégré dans divers programmes de développement de cyberarmes. Il sert à assister les développeurs dans la dissimulation de caractéristiques identifiables au sein du code source, permettant ainsi d'effacer efficacement leurs traces laissées au cours du développement. Cette démarche rappelle la modification des rayures du canon d'une arme à feu, qui dévie la trajectoire de celle-ci et complique l'enquête sur l'origine réelle de l'arme. De surcroît, ce cadre offre une fonctionnalité encore plus contestable : il permet l'insertion aléatoire de chaînes de caractères en chinois, russe, coréen, persan et arabe. Il est évident que cette fonction a été conçue pour induire en erreur les enquêteurs et imputer les cyberattaques à des pays comme la Chine, la Russie, la République populaire démocratique de Corée, l'Iran et de nombreuses nations arabes.

Comme le révèlent le code source du kit « Marble » et ses notes (Figure 1), il s'agit d'un programme de développement d'armes classé secret (à ne pas divulguer aux pays étrangers), dont le lancement n'est pas postérieur à 2015. Il est manifeste que ce programme constitue une « arme secrète » conçue par les services

de renseignement américains pour répondre à leurs propres besoins, et qu'il est même prohibé de le communiquer aux prétendus pays « alliés ».

```
/*
 * 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 : Code source du programme « Marble »

Le kit « Marble » est en mesure d'employer plus de 100 algorithmes d'obscurcissement pour substituer des contenus illisibles (non identificables) aux noms de variables intelligents et chaînes de caractères lisibles dans le fichier source, et d'y insérer des chaînes de caractères de perturbation spécifiques (Figures 2, 3, 4 et 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 : Fonction d'obscurcissement

```
#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 : Algorithme d'obscurcissement

```
{
    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 : Fonction de traitement de fichiers

```
        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 : Fonction de traitement de fichiers (suite)

Nous avons même identifié les chaînes de caractères en « langues étrangères » qui ont été délibérément intégrées dans le code source des instances de test, ces « langues étrangères » étant exclusivement l'arabe, le chinois, le russe, le coréen et le persan (Figure 6).

```
//Add foreign languages
//Arabic
WARBLE wcArabic[] = L" ﻟّﻢ أدﻳﻪ  ﻋﻴﻂ ﻧﻖ  ٣٠ ﻳﻒ  دو ل ﺎﺰﺟ ﻋﺎ  ﻟﻢ  ﺷﻞ   الك ل ﻣﺸﻠﻊ ا ﺟﻤﻞ ﻋﻤﺖ و ع ﻋﻼت ﺛﻮ ﻳﺢ غ  ﻟﻴﻀﻨﺎ ل ﻗﺶ ﻟﺎ ل ﺗﻬﻴﻦﺎ ﻟﺪ
sb.Append((LPBYTE)wcArabic, 380);


//Chinese
WARBLE wcChinese[] = L"洴浟沘 烕煓瑐 鹿楁榗 謳 鐲鑢, 篧鬔鼲 逘郠崱萑惗 澕滮湬 麔 踶輵 洋絮浽 螭螗謕 崞愊憡 榼 趏趌, 嶫 垽婖 蟷蠉螯 鏀
sb.Append((LPBYTE)wcChinese, 266);


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


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

//Farsi
WARBLE wcFarsi[] = L" ﻟﻮرم اﻳﭙﺴﻮم ﻛﻪ ﻃﺮﺡ ﻧﻤﺎ ( ﺑﻪ اﻧﮕﻠﯿﺴﯽ Lorem ipsum)  ﺑﻪ ﻣﺘﻦ آزﻣﺎﯾﺸﯽ و ﺑﯽﻣﻌﻨﯽ در  ﺻﻨﻌﺖ ﭼﺎپ  ﺻﻔﺤﻪآرا
sb.Append((LPBYTE)wcFarsi, 1710);

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

return;
```

Figure 6 : Chaînes de caractères en « langues étrangères » insérées dans le fichier

Le kit « Marble » dévoile le complot des services de renseignement américains qui mènent la

surveillance de masse sans limites en ligne à l'échelle mondiale, tout en menant l'opération « False Flag » dans l'intention d'induire en erreur les enquêteurs et les chercheurs et d'imputer ainsi ces crimes aux « pays adverses ».

L'opération « False Flag » ne se limite pas au niveau des caractéristiques du code ; en empruntant habilement les tactiques utilisées par des groupes de cybercriminalité, les services de renseignement américains créent à merveille une variété d'« organisations fictives », comme cela a été détaillé dans notre deuxième rapport. Ainsi, les forces de cyberguerre et les hackers des services de renseignement des Etats-Unis se comportent tels des caméléons dans le cyberespace, qui changent d'identité et d'apparence à leur guise, « représentent » d'autres nations pour mener des cyberattaques et des campagnes d'espionnage, tout en imputant ces crimes aux pays non « alliés » des Etats-Unis.

Selon des sources fiables, l'opération « False Flag » constitue en réalité un élément clé de l'opération « Effects » menée par les services de renseignement américains. Les documents confidentiels des Etats-Unis et des pays membres de l'alliance des « Five Eyes » révèlent que l'opération « Effects » comprend essentiellement deux volets : la désinformation et le brouillage. La NSA a élaboré un manuel d'application pour ce dernier, dont l'opération « False Flag » représente une partie importante. Par ailleurs, ces documents confidentiels soulignent les quatre principes fondamentaux à respecter pour mener à bien l'opération « Effects », à savoir : déni, brouillage, diffamation et tromperie. Ces quatre principes englobent précisément tous les éléments essentiels de l'opération « Volt Typhoon » (Figures 7 et 8).

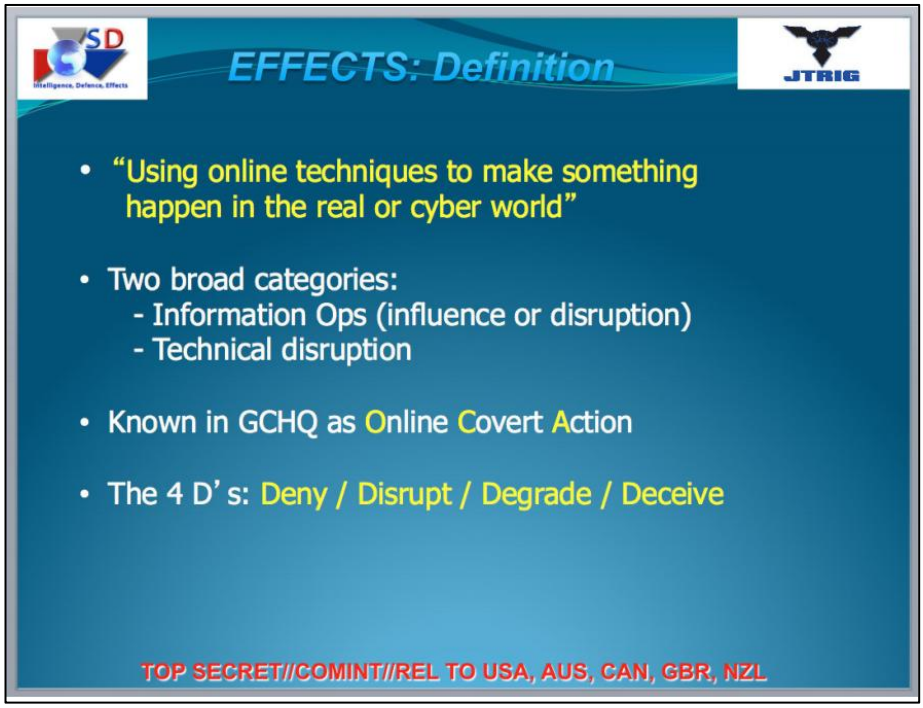


Figure 7 : Définition de l'opération « Effects » par les Etats-Unis et les pays membres de l'alliance des « Five Eyes »

Figure 8 : Manuel d'application du brouillage mené par les Etats-Unis et les pays membres de l'alliance des « Five Eyes »

A partir des preuves susmentionnées, on peut conclure que l'opération « Volt Typhoon » constitue une typique opération de désinformation (à savoir l'opération « False Flag ») soigneusement orchestrée et au service des groupes d'intérêt américains. Les tactiques employées dans cette opération coïncident parfaitement avec celles pratiquées par les services de renseignement des Etats-Unis et des pays membres de l'alliance des « Five Eyes » dans le cadre de l'opération « Effects ». Il est manifestement ardu de déjouer ce stratagème minutieusement élaboré par les services de renseignement américains, car, face à une multitude d'informations perturbatrices, l'analyse technique seule s'avère insuffisante. Il est impératif d'effectuer une analyse synthétique des diverses sources d'informations et des documents concernés afin de découvrir les négligences et erreurs qu'ils ont, sans le vouloir, révélées. Cela permettra ainsi de comprendre et d'interpréter correctement les plans sinistres conçus par la NSA, la CIA et d'autres services de renseignement. Ce sont les efforts que nous avons déployés derrière nos deux rapports d'enquête précédents (voir « Volt Typhoon : Une campagne d'escroquerie menée par les services de renseignement américains contre le Congrès et les contribuables américains» et « Volt Typhoon II : Une campagne de désinformation menée par les agences du gouvernement fédéral américain contre le Congrès et les contribuables américains »).

III. « Espions » du cyberespace

Dans notre deuxième rapport, nous avons rendu public le scandale politique des agences du gouvernement fédéral américain, et plus particulièrement de leurs services de renseignement, qui avaient inventé des menaces issues des réseaux extérieurs et orchestré la désinformation, afin de préserver leur droit de surveillance sans mandat accordé par la section 702 du Foreign Intelligence Surveillance Act (FISA), et

de maintenir leur vaste programme de surveillance de masse sans limites. Le présent rapport en exposera les détails.

1. Serrer la « gorge » d'Internet

D'après des informations *top secret* de la NSA (Figure 9), les Etats-Unis tirent parti de leur avantage technologique et géographique dans le déploiement de réseaux Internet pour exercer un contrôle rigoureux sur les câbles à fibre optique au fond de l'Atlantique et du Pacifique, qui représentent les principales voies de communication de l'Internet, pour établir successivement sept stations d'écoute nationales à flux total, analyser en profondeur les protocoles et s'approprier les données transmises par ces câbles, en étroite collaboration avec le Bureau fédéral d'enquête (FBI) aux Etats-Unis et le Centre national de cybersécurité (NCSC) au Royaume-Uni, et procéder à une surveillance de masse auprès des internautes du monde entier.

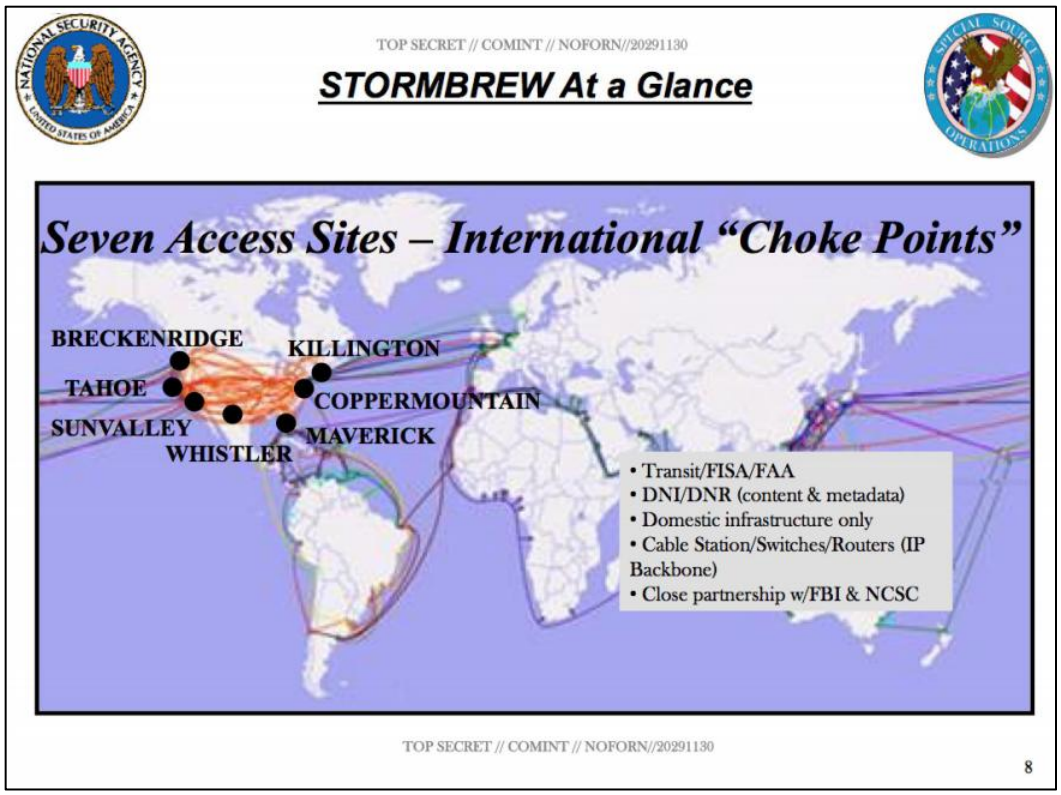


Figure 9 : Stations d'écoute établies par la NSA

Les bénéficiaires de ces informations d'écoute et de renseignement sont nombreux. En plus des services de renseignement et des agences militaires des Etats-Unis, un grand nombre de services administratifs du gouvernement fédéral américain, y compris la Maison Blanche, le Cabinet, les ambassades des Etats-Unis à l'étranger, le Bureau du Représentant au commerce des Etats-Unis (USTR), le Congrès, ainsi que le Département d'Etat, les ministères de l'Agriculture, de la Justice, du Trésor, de l'Energie, du Commerce et de la Sécurité intérieure. Comme nous l'avons souligné dans notre deuxième rapport, les acteurs du programme « Volt Typhoon » ne se limitent pas aux services de renseignement américains ; de nombreuses agences du

gouvernement fédéral américain jettent de l'huile sur le feu, dans le but de servir les intérêts collectifs des groupes d'intérêt (Figure 10).

Figure 10 : « Clients » des renseignements de la NSA

2. « Réservoir » des données Internet

La surveillance doit aboutir inévitablement à une multitude d'informations et données lisibles. Il en découle qu'il est essentiel pour la NSA de traduire et de transformer en temps réel le flux de transmission dans les câbles sous-marins à fibre optique en informations de renseignement lisibles et exploitables. Avec l'augmentation des flux de données cryptées, cette tâche s'est révélée de plus en plus ardue. Pour y faire face, la NSA a initié deux projets majeurs : le projet « UpStream », qui vise à conserver l'intégralité des données brutes des câbles sous-marins à fibre optique interceptées par les stations d'écoute, créant ainsi un vaste réservoir de données servant de point de départ pour un traitement ultérieur des informations de renseignement ; et le projet « Prism », dont l'objectif est de classifier les données de communication brutes provenant du projet « UpStream » en fonction des applications Internet et d'analyser leur contenu. En outre, afin de résoudre les problèmes majeurs liés au décodage des données cryptées et à la couverture insuffisante des flux de communication dans le projet « UpStream », le gouvernement américain a imposé au projet « Prism » d'accéder directement aux serveurs des grandes entreprises Internet du pays, telles que Microsoft, Yahoo, Google, Facebook (aujourd'hui Meta) et Apple, pour récupérer ainsi les données des utilisateurs. Ces deux projets ont été mis en œuvre sous l'autorisation accordée par la section 702 du FISA, qui est devenue

l'argument officiel des services de renseignement américains pour justifier leur interception légitime, ouverte et continue de données transmises à travers les câbles Internet mondiaux au nom du gouvernement fédéral américain. Cela constitue également une preuve probante et indéniable que les Etats-Unis incarnent un empire de la surveillance (Figure 11).

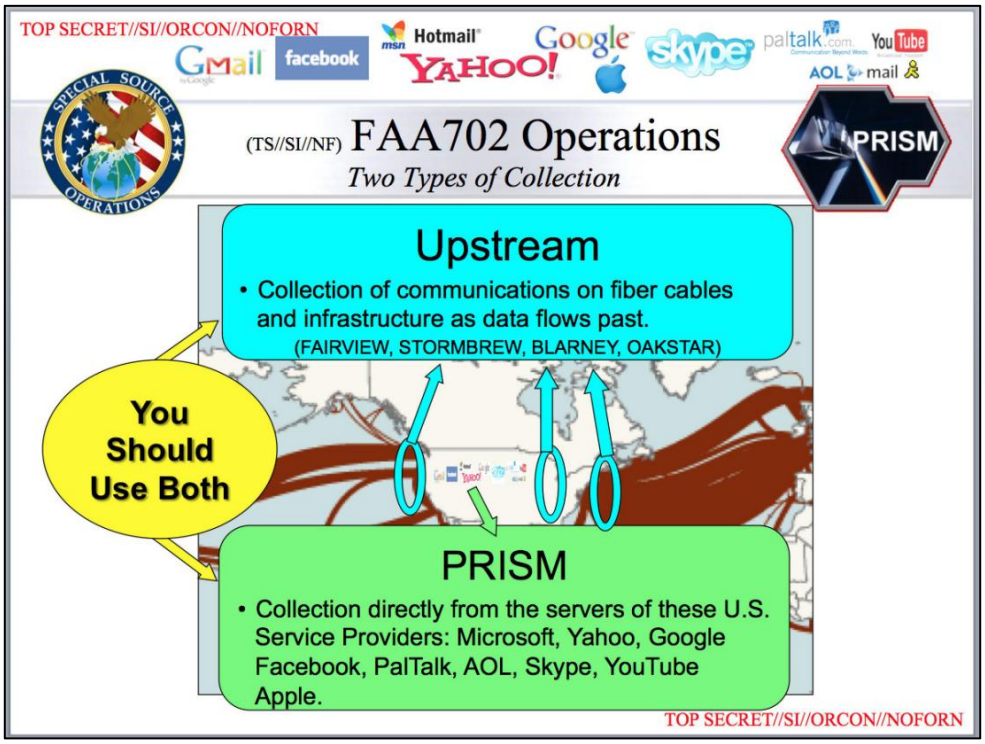


Figure 11 : Les deux projets d'écoute de la NSA

3. Cyberintrusion jusqu'à la source des données

Bien que la NSA ait établi un vaste réseau d'écoute sur Internet à l'échelle mondiale, ses systèmes, concentrés sur certaines zones spécifiques couvertes par les câbles sous-marins, n'ont pas permis de recueillir suffisamment de données pour satisfaire ses besoins en information. Pour remédier à cette lacune, la NSA a mené la cyberintrusion CNE (Computer network exploitation), ciblant les objectifs situés dans des zones aveugles à ses systèmes d'écoute. C'est dans ce cadre que le bureau des Opérations d'accès sur mesure (TAO), le fameux service de la NSA très controversé, a été mobilisé pour accomplir cette tâche délicate. D'après des documents *top secret* de la NSA, le TAO a mené l'opération CNE à l'échelle mondiale sans distinction et a déployé plus de 50 000 implants. Les cibles se situent principalement en Asie, en Europe de l'Est, en Afrique, au Moyen-Orient et en Amérique du Sud. Les documents internes de la NSA révèlent que presque toutes les grandes villes chinoises sont dans le viseur de cette opération. De nombreux actifs Internet ont déjà été compromis, y compris ceux de l'Université polytechnique du Nord-Ouest de la Chine et ceux liés au Centre de surveillance sismique de Wuhan. La plupart des centres de commandement de ces programmes d'espionnage se trouvent dans les bases militaires situées en dehors du territoire américain, y compris celles au Japon, en République de Corée, à Guam et à Hawaï. Guam ne devrait pas être étranger à ceux ayant suivi

nos deux rapports précédents. On pourrait le considérer comme le foyer de la désinformation « Volt Typhoon » du gouvernement américain. Il s'inscrira dans les annales de la cybersécurité en raison de ce récit fallacieux. En réalité, la base militaire américaine à Guam, au lieu d'être la victime des cyberattaques « Volt Typhoon », est l'origine de nombreuses cyberattaques contre la Chine et beaucoup de pays d'Asie du Sud-Est, ainsi que le centre de collecte de données interceptées (Figures 12 et 13).

Pour certaines cibles de grande valeur dans d'autres pays avec un niveau de protection élevé et difficiles d'accès, le TAO adopte directement l'attaque des chaînes d'approvisionnement. Cette stratégie tire profit de l'avantage des Etats-Unis en matière de technologies et de produits avancés de cybersécurité. En collaboration avec les géants du Web ou les grands fournisseurs d'équipements américains, le TAO intercepte, au niveau des canaux de livraison et de logistique, les équipements Internet américains achetés par les cibles ou par leurs fournisseurs de services d'accès à Internet. Par la suite, ces appareils sont démontés, réemballés après l'implantation de portes dérobées, et expédiés vers les cibles d'attaque. Cette tactique est généralement utilisée pour cibler les opérateurs de télécommunications et d'Internet étrangers, permettant ainsi de prendre le contrôle de leurs systèmes de facturation. Cela ouvre la voie à l'écoute des communications mobiles des individus ciblés. Dans le cadre de la cyberattaque lancée par le TAO contre l'Université polytechnique du Nord-Ouest de la Chine, un opérateur de télécommunications et d'Internet basé sur le territoire chinois a été la cible de cette attaque. Les contenus des appels, les activités en ligne et le suivi des actions réelles des cibles ont été espionnés en templs réel par le TAO (Figure 14).

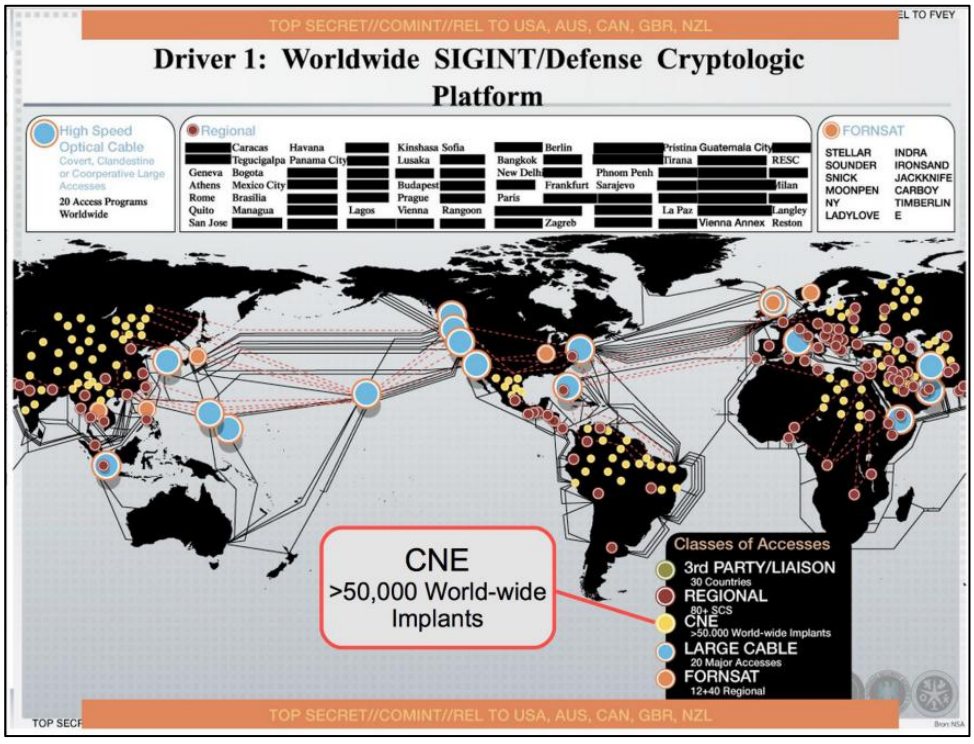


Figure 12 : Schéma de l'opération CNE menée par le TAO

Figure 13 : Schéma de l'intrusion du TAO dans les réseaux d'Internet chinois

Figure 14 : Des techniciens du TAO démontent des équipements Internet de Cisco Systems achetés par la cible d'écoute et y implantent des portes dérobées

Il est surprenant que la NSA emploie le terme tactique de « prépositionnement » pour qualifier cette attaque à travers les chaînes d'approvisionnement, qui consiste à implanter des portes dérobées informatiques dans les produits Internet destinés à la cible, en vue de mener des opérations d'espionnage et de contrôle

éventuelles. Nous avons également noté que le terme « prépositionnement » est utilisé par le gouvernement fédéral américain pour décrire les tactiques supposément mises en œuvre par le groupe « Volt Typhoon » lors des cyberattaques visant les infrastructures clés américaines situées à Guam et ailleurs. Qui a adopté la tactique de prépositionnement dans les infrastructures clés situées à travers le monde ? La réponse est claire.

4. Recherche abusive des renseignements Internet

Sous l'autorisation accordée par la section 702 du FISA, les services de renseignement américains ont établi un vaste réseau de surveillance sur Internet, fournissant au gouvernement américain une quantité considérable de renseignements de grande valeur. Cela permet à celui-ci de maintenir régulièrement un avantage dans les domaines diplomatique, militaire, économique et scientifique. La section 702 et le système de surveillance Internet qui lui est associé sont devenus des « armes secrètes » essentielles des Etats-Unis pour préserver leur statut de puissance hégémonique à l'heure actuelle. Fort de cet avantage technologique privilégié, le gouvernement fédéral américain et ses services de renseignement agissent de plus en plus sans retenue, n'hésitant pas à surveiller n'importe quelle cible. En voici quelques exemples, preuves à l'appui.

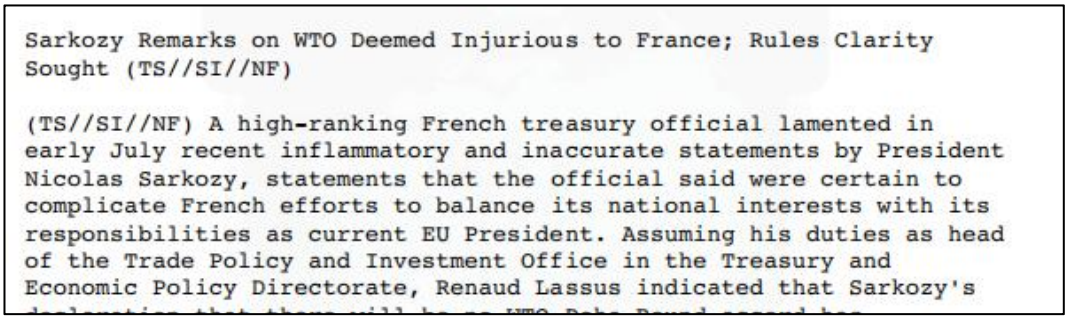
A. La France

Entre 2004 et 2012, les Etats-Unis ont mené contre la France l'espionnage, englobant divers domaines tels que les politiques gouvernementales, la diplomatie, les finances, les échanges internationaux, la construction d'infrastructures, ainsi que les activités commerciales. Certaines de ces informations de renseignement ont été partagées, sous l'autorisation des Etats-Unis, avec les pays membres de l'alliance des « Five Eyes », ce qui indique que même ces derniers sont les bénéficiaires des opérations d'espionnage américaines. Les renseignements de surveillance associés à cette opération ont permis aux Etats-Unis d'intercepter des communications provenant de secteurs politiques et économiques clés de France, y compris la résidence présidentielle. Dans les documents *top secret* des services de renseignement américains rendus publics, on peut trouver plusieurs résumés d'informations confidentielles obtenues à l'aide de l'écoute des conversations et des communications de hauts fonctionnaires du gouvernement français, tels que l'ancien Président français, les ministres des Finances et des Affaires étrangères, des sénateurs, des responsables de la direction générale des politiques financières et économiques, des ambassadeurs de France aux Etats-Unis, ainsi que des responsables en charge de la politique commerciale de l'Union européenne, entre autres.

Le contenu de ces renseignements concerne les politiques et les considérations internes du gouvernement français vis-à-vis de l'Organisation mondiale du commerce, de l'Accord de Partenariat transpacifique, du G7 et du G20, ainsi que le budget du gouvernement français, le déclin de l'industrie automobile française et la participation des entreprises françaises dans le programme « Oil-for-Food ».

Il a été clairement ordonné de rassembler, dans le cadre de l'espionnage économique susmentionné, toutes les données relatives aux ventes et au financement des projets majeurs touchant aux secteurs des télécommunications, de l'électricité, du gaz naturel, du pétrole, de l'énergie nucléaire, des énergies renouvelables, ainsi qu'aux technologies environnementales et médicales en France. Par ailleurs, il a également été ordonné d'intercepter (ou de dérober) tout contrat ou transaction d'une valeur supérieure à 200 millions de dollars américains impliquant des sociétés françaises, ce qui a des répercussions directes sur les grandes entreprises telles que BNP Paribas, AXA, Crédit Agricole, Peugeot, Renault, Total et Orange, ainsi

que les principaux groupements agricoles du pays. Le résumé des informations confidentielles espionnées par la NSA dans le cadre de son opération d'espionnage contre la France est présenté dans le tableau 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 : Enregistrements de la surveillance menée par la NSA contre l'ancien Président français Nicolas Sarkozy

Tableau 1. Compte-rendu partiel des renseignements de surveillance de la NSA contre les membres du gouvernement français

Date	Classement de renseignements	Contenu
2004	Renseignement sur l'ambassadeur de France à Washington	L'ambassadeur de France à Washington envisge de publier une liste d'entreprises américaines bénéficiaires du programme Oil-For-Food (OFF).
2006	Communications entre les dirigeants de haut niveau du gouvernement français	Le président Jacques Chirac échange des idées avec son ministre des Affaires étrangères sur le sujet des nominations à l'ONU.
2008	Communications entre les dirigeants de haut niveau du gouvernement français	Le directeur général des politiques financières et économiques exprime son mécontentement à l'égard des propos du président Nikolas Sarkozy sur l'éventuel impact négatif des négociations avec l'OMC.
2008	Communications entre les dirigeants de haut niveau du gouvernement français	Le président Nicolas Sarkozy impute aux Etats-Unis la crise économique mondiale, déclarant que la France s'engagera en premier dans la réforme du système financier mondial.

Date	Classement de renseignements	Contenu
24 mars 2010	Communications entre les dirigeants de haut niveau du gouvernement français	Communications entre l'ambassadeur de France à Washington et le conseiller des affaires étrangères du président Sarkozy : celui-ci envisage d'aborder lors de sa rencontre avec le président américain Obama, prévue le 31 mars 2010, des sujets sensibles tels que le retrait des Etats-Unis de l'Accord de coopération bilatérale de renseignement (cet accord devrait imposer aux Etats-Unis des restrictions dans la surveillance contre la France) ; la France promettrait de fournir à l'Afghanistan des avions d'entraînement militaires ; l'European Aeronautic Defence and Space Company (EADS) signerait avec l'armée américaine un contrat d'avions ravitailleurs ; le différend autour de la marque du groupe français de spiritueux Pernod Ricard.
10 juin 2011	Communications entre les dirigeants de haut niveau du gouvernement français	Communications entre le président Sarkozy et son ministre des Affaires étrangères : Sarkozy fait des remarques durcies sur le sujet Israël-Palestine.
2 août 2011	Communications entre les dirigeants de haut niveau du gouvernement français	Communications entre les fonctionnaires français et européens basés à Washington : ils critiquent vivement les politiques commerciales des Etats-Unis, déclarant que l'Accord de Partenariat transpacifique (TPP) est un accord contre la Chine.
22 mai 2012	Communications entre les dirigeants de haut niveau du gouvernement français	Le gouvernement français s'inquiète de l'impact de la crise de la dette dans la zone euro, notamment du retrait de la Grèce de la zone euro, sur la France et sur les entreprises françaises. Mécontent de l'attitude intransigeante de la chancelière allemande Angela Merkel, le président François Hollande accepte de la contourner pour rencontrer en secret des membres des partis d'opposition allemands.
31 juillet 2012	Communications entre les dirigeants de haut niveau du gouvernement français	Conversations entre le ministre des Finances et un sénateur français : le premier estime que l'économie française, qui s'enlise, devrait rencontrer de grandes difficultés dans les deux ans à venir.
2012	Ordonnance concernant la surveillance américaine à l'encontre de la France	L'ordonnance exige un espionnage durable sur la France afin d'obtenir des informations liées aux activités des entreprises françaises, aux politiques et décisions économiques du gouvernement français. L'ordonnance aborde également des sujets tels que les relations économiques entre la France, les Etats-Unis, d'autres pays ainsi que des institutions économiques internationales, les politiques financières et commerciales du gouvernement français, la position de la France sur l'agenda du G8 et du G20.

Date	Classement de renseignements	Contenu
2012	Ordonnance concernant la surveillance américaine à l'encontre de la France	L'ordonnance demande à ses espions de collecter toutes les informations de la France concernant les ventes et le financement liés aux grands projets dans les secteurs tels que la télécommunication, la production d'électricité, le pétrole, l'énergie nucléaire, les énergies renouvelables, l'environnement et la santé. L'ordonnance demande à ses agents d'intercepter et de transmettre à l'échelon supérieur tous les contrats et négociations des entreprises françaises dont la valeur dépasse 200 millions de dollars.
2012	Agenda de réunions des fonctionnaires du gouvernement français	Le ministère français des Finances a rédigé pour son ministre un discours qui sera prononcé lors des sommets du G7 et du G20. Selon le discours, la France exhortera les Etats-Unis à mener des réformes bancaires et soutiendra l'initiative des Etats-Unis sur les réserves pétrolières stratégiques.

B. L'Allemagne

Selon les documents confidentiels de la NSA, le service fédéral de renseignement allemand BND et l'Office pour la protection de la Constitution BfV ont coopéré à plusieurs reprises avec les services de renseignement américains pour mener des opérations de surveillance en Europe, y compris en Allemagne[3]. Ils ont même, de concert avec la CIA, acquis Crypto AG, une société de cryptotechnologie basée en Suisse, pour offrir aux cibles de surveillance des produits crypto équipés de portes dérobées[4]. Malgré tout cela, les Etats-Unis ont exclu l'Allemagne de l'alliance des « Five Eyes », la considérant comme un partenaire de troisième niveau. Pour les Etats-Unis, l'Allemagne est à la fois un partenaire et une cible de surveillance.

En réalité, les armées américaines de terre, de l'air et de mer ainsi que la NSA ont créé en Allemagne un grand nombre de stations d'information visant à surveiller l'Allemagne et d'autres pays européens (Figure 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

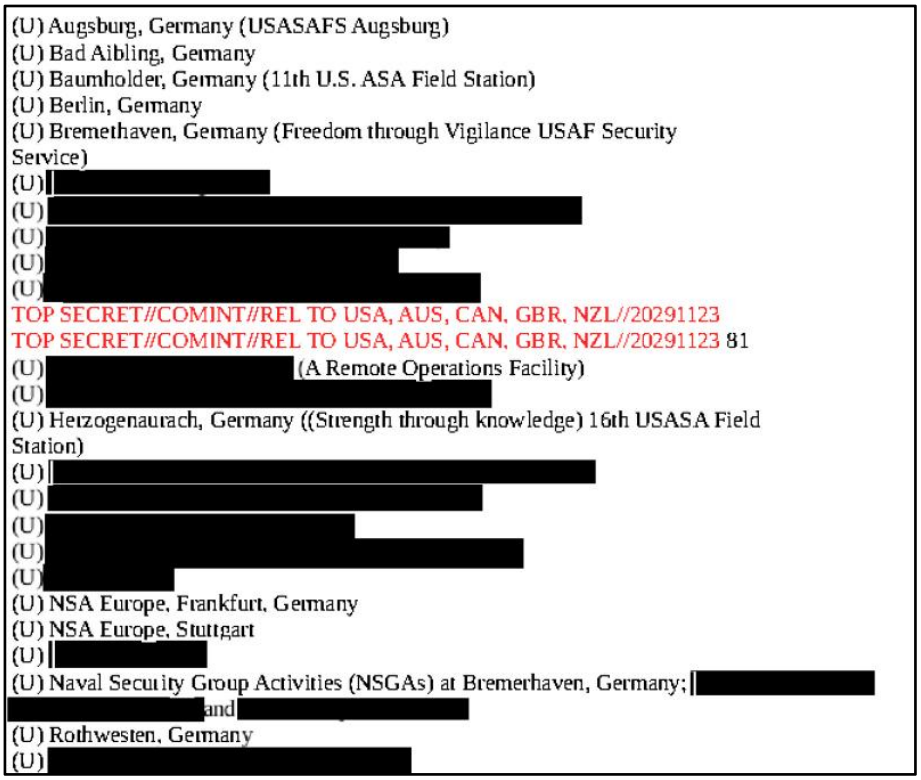
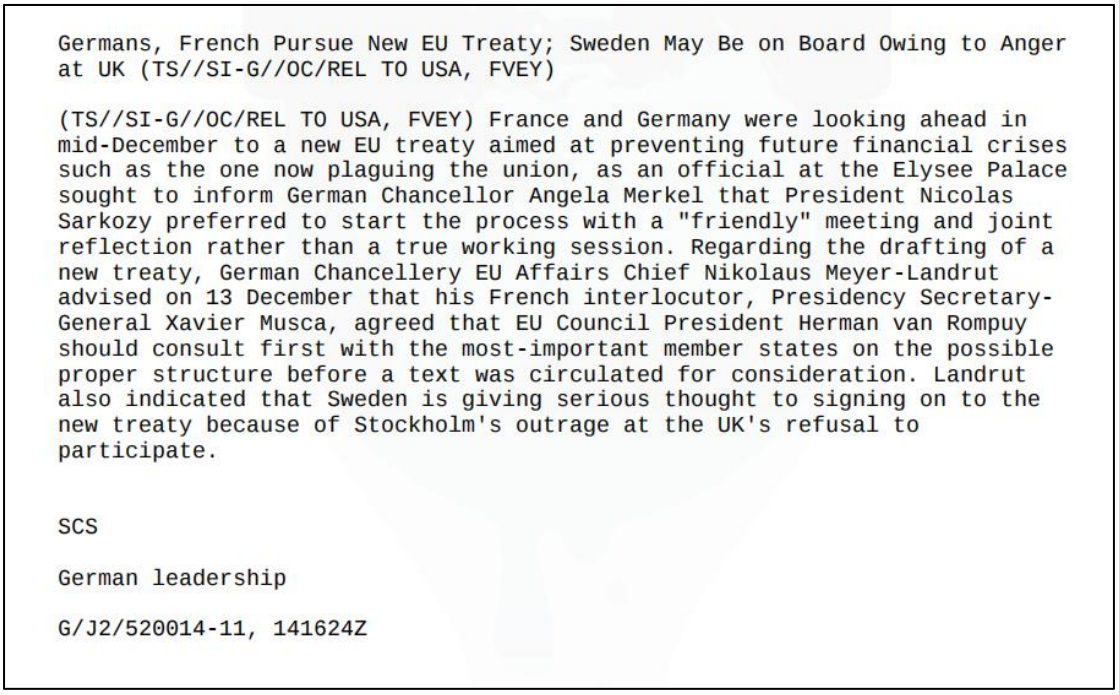

(U) Augsburg, Germany (USASAFS Augsburg)
(U) Bad Aibling, Germany
(U) Baumholder, Germany (11th U.S. ASA Field Station)
(U) Berlin, Germany
(U) Bremethaven, Germany (Freedom through Vigilance USAF Security Service)
(U) [redacted]
(U) [redacted]
(U) [redacted]
(U) [redacted]
(U) [redacted]
TOP SECRET//COMINT//REL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

Figure 16 : Stations d'information établies en Allemagne par les services de renseignement américains

La NSA surveille depuis longtemps les communications des fonctionnaires allemands de haut niveau, dont notamment la chancelière, le ministre des Affaires étrangères, des ambassadeurs et des consuls à l'étranger. La surveillance couvre un large éventail de sujets, dont l'opinion du gouvernement allemand sur la situation internationale et les incidents d'urgence, ainsi que les discussions confidentielles des fonctionnaires allemands impliquant des sujets politiques, militaires, économiques, diplomatiques, ethniques, sécuritaires, des ressources, etc. Il est à noter que les Etats-Unis s'intéressent beaucoup aux dossiers de l'Union européenne, notamment à la solution des risques financiers (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

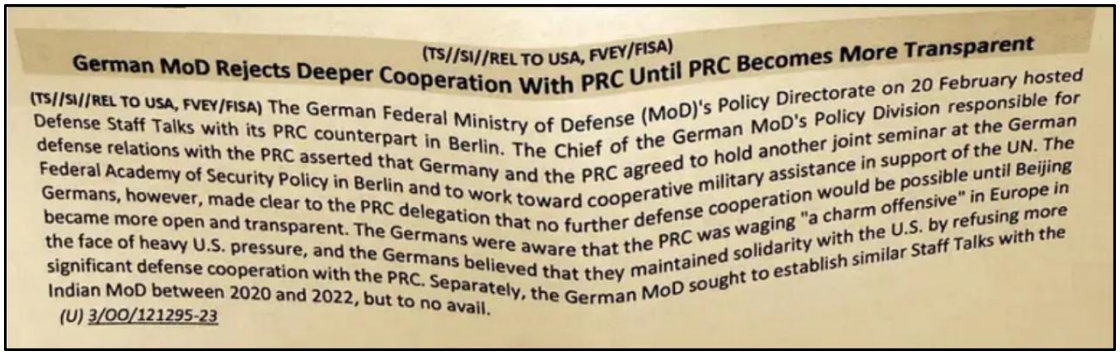
Figure 17 : Enregistrement de surveillance de la NSA contre les dirigeants du gouvernement allemand

Même après l'affaire Snowden, les Etats-Unis n'ont pas relâché leur surveillance contre l'Allemagne. Ils ont adopté une approche plus secrète. En mai 2021, les médias danois[5] ont dévoilé la coopération entre la NSA et le service danois de renseignement militaire extérieur FE visant à surveiller les câbles Internet à fibre optique passant par le Danemark. Chefs d'Etat, politiciens et fonctionnaires de haut niveau allemands, suédois, norvégiens et français sont tous des cibles. La chancelière allemande Angela Merkel, le ministre allemand des Affaires étrangères Frank-Walter Steinmeier et le chef de l'oppositon Peer Steinbrük ont tous été surveillés. Le président américain Joe Biden, alors vice-président, était en charge de ce projet de surveillance.

Cette opération de surveillance, une fois dévoilée par les médias, a suscité le mécontentement de l'Allemagne, de la France et d'autres pays d'Europe. La chancelière allemande Angela Merkel et le président français Nikolas Sarkozy ont affirmé que la surveillance des Etats-Unis contre les alliés était « inacceptable ». Evidemment, le mécontentement des alliés a été totalement ignoré par les Etats-Unis. En avril 2023, la surveillance américaine contre le ministère allemand de la Défense a été de nouveau exposée[6].

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

[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.

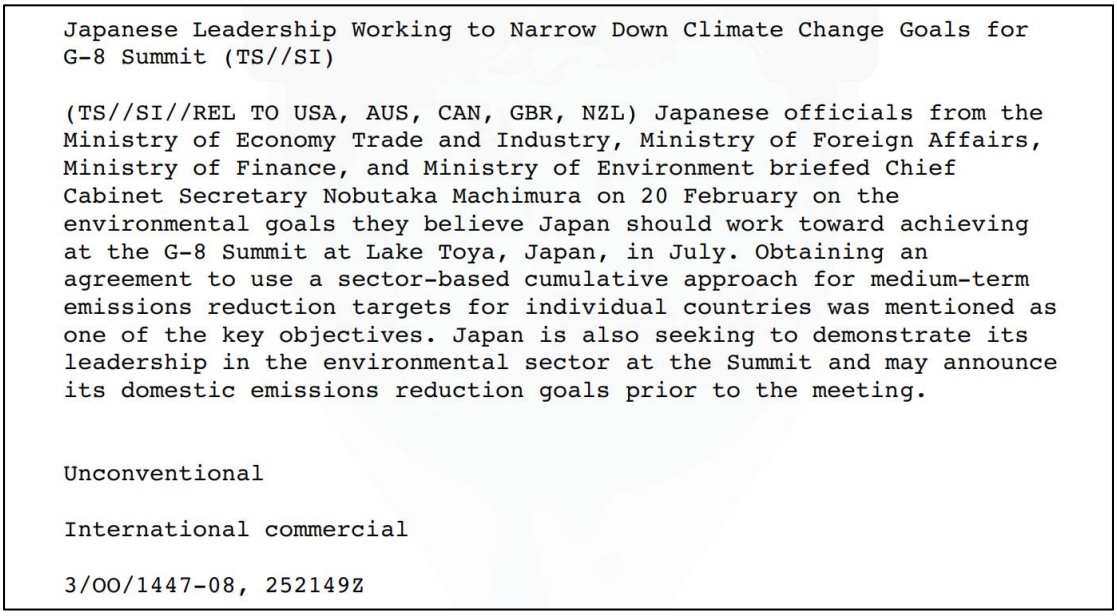
(U) 3/OO/121295-23

Figure 18 : Enregistrement de surveillance de la NSA contre le ministère allemand de la Défense

Comme le montrent les documents *top secret* de la NSA (Figure 18), un dialogue militaire et diplomatique entre le ministère allemand de la Défense et une délégation du ministère chinois de la Défense, qui a eu lieu le 20 février 2023, a été surveillé. Les Etats-Unis étaient particulièrement préoccupés par l'opinion et la position de l'Allemagne dans la coopération militaire avec la Chine.

C. Le Japon

La banque de données d'écoute de la NSA comprend une liste de cibles politiques et économiques japonaises. Selon cette liste, la surveillance américaine contre le Cabinet japonais ainsi que les ministères et les groupes financiers japonais remonte à l'administration Shinzo Abe. Les standards téléphoniques dans les bureaux du Cabinet, l'adjoint administratif du secrétaire général du Cabinet Yoshihide Suga, de nombreux fonctionnaires de la banque centrale, le département du gaz naturel de Mitsubishi Corporation et le département du pétrole de Mitsui & Co., etc., ont tous été des cibles de surveillance. Un document intitulé « Projet secret du Japon sur le changement climatique à publier lors du Sommet du G8 » (Figure 19) porte la mention « REL TO USA, AUS, CAN, GBR, NZL », ce qui signifie que cette information a été partagée, sous l'autorisation américaine, avec les pays membres de l'alliance des « Five Eyes ». Ces informations auraient été volées aux services du gouvernement japonais, dont le contenu concerne divers sujets, tels que le conflit commermcial autour de produits agricoles, la position du Japon au cycle de Doha sous l'égide de l'OMC, les politiques pour faire face au changement climatique, les politiques liées à l'énergie nucléaire, le plan d'émission de carbone, les communications entre le Japon et des institutions internationales, dont l'Agence internationale de l'énergie (IEA), ainsi que des réunions qui se tiennent dans la résidence du Premier ministre Shinzo Abe.



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 : Enregistrement de surveillance de la NSA contre les dirigeants japonais

D. Citoyens américains

Comme nous l'avons révélé dans notre deuxième rapport, il y a aux Etats-Unis une forte opposition contre la section 702. Conformément à celle-ci, la NSA et les autres services de renseignement américains ne surveillent que les étrangers en dehors des Etats-Unis. Mais comme le montre la feuille de route technologique de la NSA, la surveillance vise à obtenir de manière illégale toutes les données de communication des internautes du monde entier, dont les citoyens américains sur le territoire américain. Les services de renseignement américains, dont la NSA, exigent à leurs agents d'éviter « autant que possible », lors de la configuration des conditions de choix, de cibler les citoyens américains sur le territoire des Etats-Unis et vivant à l'étranger. Mais cette mesure, qui repose presque entièrement sur l'autodiscipline, est en réalité vaine. La cour FISA (United States Foreign Intelligence Surveillance Court) a révélé le 19 mai 2023 un dossier[7], mettant en lumière des milliers d'infractions à la section 702 (Figure 20). Selon ce dossier, le FBI a abusé à plusieurs reprises des outils de surveillance, en mettant en écoute les citoyens américains impliqués dans l'assaut du Capitole à Washington le 6 janvier 2021 et dans les protestations de « Black Lives Matter » en 2020. Ce dossier a été exposé et remis en cause par les médias[8]. En réalité, le FBI, la NSA et la CIA ont effectué une surveillance de masse contre tous les participants du mouvement « Occupy Wall Street » et leurs correspondants. Cette approche a ensuite été utilisée dans le « Mouvement Tournesol des Etudiants » à Taïwan et dans les rassemblements illégaux « Occupy Central with Love and Peace » à Hong Kong. Tout cela montre que les services de renseignement américains n'ont cessé de surveiller leurs propres citoyens.

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

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

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

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

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

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

Figure 20 : Infractions à la section 702 publiées par la cour FISA

Un tel abus des outils de surveillance est dû à l'attitude du laisser-faire des services de renseignement américains qui ferment leurs yeux aux infractions à la section 702 (Figure 21). Un matériel de formation en interne des services de renseignement américains a clairement indiqué que si les analystes du renseignement découvrent « par hasard » des informations personnelles des citoyens américains au cours de leur travail, cela ne constitue pas une violation et ne nécessite pas un signalement.

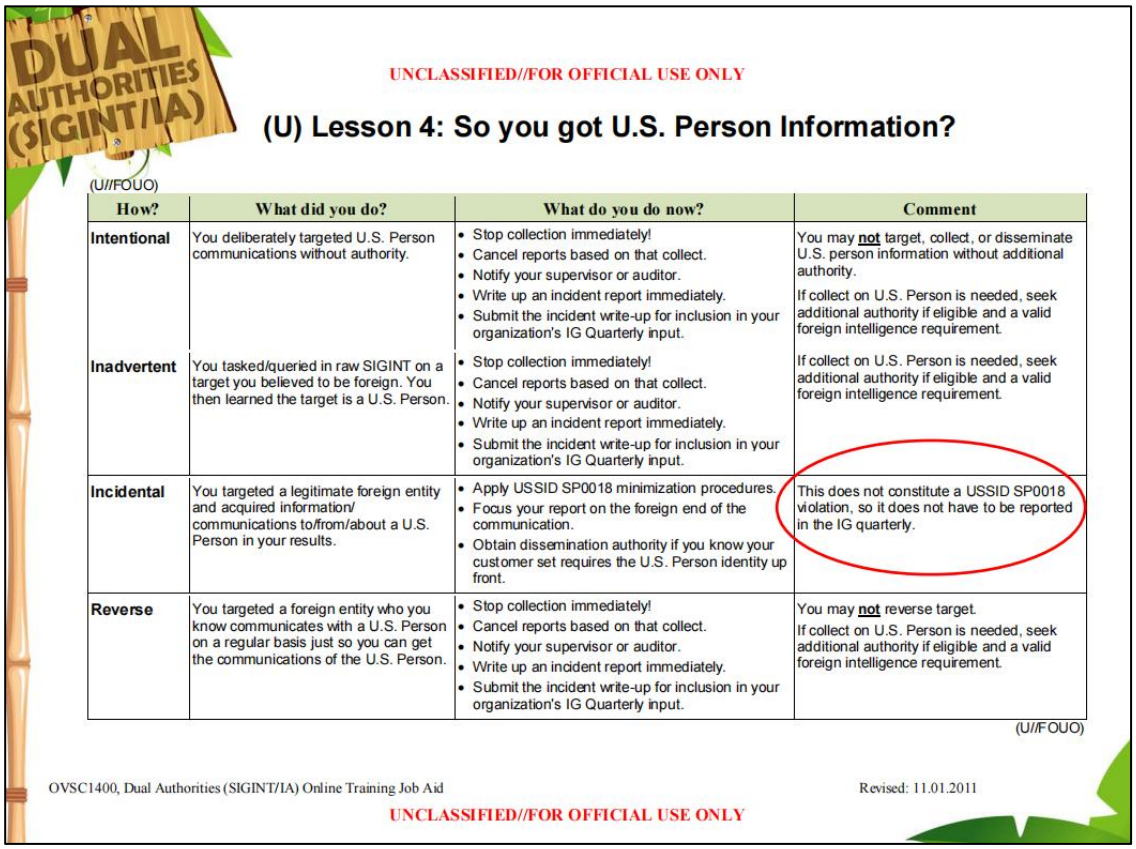


Figure 21 : Matériel de formation en interne des services de renseignement américains concernant la section 702

Les nombreuses stations de surveillance dans le cadre de la surveillance américaine des réseaux Internet sont comme des « espions » omniprésents dans le réseau Internet, qui surveillent en temps réel les données des utilisateurs d'Internet du monde entier. Cela constitue pour les Etats-Unis la base indispensable pour construire leur « Matrix » d'espionnage. Un programme de surveillance tellement immense nécessite un investissement colossal, qui ne cesse d'augmenter avec la croissance explosive des données Internet. C'est la raison principale pour laquelle le gouvernement fédéral des Etats-Unis et ses services de renseignement fabriquent l'affaire « Volt Typhoon ».

Nombreux sont les politiciens américains qui trompent le Congrès pour leurs propres gains personnels. Christopher Wray, directeur du FBI, qui a joué un rôle important dans le récit fallacieux du projet « Volt Typhoon », est un menteur récidiviste. En juillet 2022, Christopher Wray et le procureur général des Etats-Unis, Merrick Garland, ont été interrogés par le Sénat pour avoir dissimulé les preuves criminelles du fils du président américain Joe Biden[9]. En août 2023, Christopher Wray a de nouveau été interrogé par le Sénat pour avoir fourni au Congrès de faux mémorandums[10]. En juillet 2024, il s'est parjuré devant le Congrès, déclarant que Donald Trump n'a pas été touché par une balle[11]. Il a également dissimulé le véritable état de santé de Joe Biden. Donald Trump a réclamé avec force la démission de Christopher Wray.

IV. Démentis

Après la publication de notre deuxième rapport sur le « Volt Typhoon », les services officiels et les principaux médias des Etats-Unis restent silencieux, tandis que certains fonctionnaires du gouvernement américain, anciens ou actuellement en poste, ainsi qu'une partie d'entreprises de cybersécurité américaines, ont exprimé leurs points de vue sur les réseaux sociaux, sur des médias spécialisés dans la cybersécurité et sur des médias indépendants. Certains ont déclaré, d'une voix « coordonnée », que notre rapport a « déformé » et « abusé » les résultats de recherche des entreprises américaines, qui se sont hâtées de réclamer qu'elles « n'avaient aucun lien » avec le rapport. Il faut souligner que notre pratique, qui consiste à citer et à faire référence aux résultats de recherche d'autres établissements, est conforme aux pratiques habituelles du secteur. Nous avons été accusés de « déformer » et d'« abuser » ces recherches juste parce que nous sommes arrivés à une conclusion différente. Nous nous sommes rendus compte de l'hégémonie américaine sur Internet et nous sommes encore plus convaincus que ces entreprises américaines avaient dû prendre position à cause de pressions extérieures.

Le reniement de ThreatMon mérite réflexion. Cette société a déclaré lors d'une interview qu'elle a modifié les statistiques de son rapport originel à cause des erreurs en matière d'indicateur d'infection. Une telle explication purement formelle inspire le scepticisme. Sans parler du moment de la révision, la page

[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

qu'elle a retirée recelait en fait des preuves clés telles que des adresses IP, des adresses de serveurs de commandes ainsi que des adresses des portefeuilles de crypto-monnaie. Toutes ces donnnées ont-elles été mal tournées pendant le processus de la collecte ? Où sont alors la scientificité, l'aptitude et la qualité technologiques de ThreatMon ? S'aligner sur d'autres établissements « dociles » sous pression du gouvernement américain constitue-t-il son esprit académique ? Si les recherches de suivi ont été menées de manière rigoureuse, n'est-il pas nécessaire d'ajouter une explication dans le rapport modifié ? N'est-il pas nécessaire de modifier en même temps le sommaire ? La pratique inhabituelle de ThreatMon suppose que la révision du rapport est faite à la hâte sous l'énorme pression extérieure. Dans notre nouveau rapport, nous avons fourni davantage de preuves qui confirment de manière indéniable que les services de renseignement américains surveillent contre la Chine, la Russie, l'Iran et les pays arabes et qu'ils donnent de fausses informations au Congrès et aux contribuables américains.

La réaction de Microsoft mérite également notre attention. Sherrod DeGrippo, directeur de la stratégie de renseignement sur la menace chez Microsoft, a déclaré lors du Black Hat du 11 août 2024 que le groupe « Volt Typhoon » était toujours actif sans montrer aucun signe d'arrêt. Pourtant Microsoft n'a livré aucune preuve solide pour confirmer que le groupe « Volt Typhoon » a un lien avec le gouvernement chinois. En fait, depuis 2023, de nombreuses pratiques de Microsoft éveillent des suspects. Comme nous l'avons indiqué dans les deux rapports précédents, Microsoft a renforcé considérablement la coopération avec l'armée et les services de renseignement américains. En 2024, cette coopération a encore été approfondie. Selon un article de Bloomberg[12] publié le 7 mai 2024, Microsoft a déployé pour les services de renseignement américains des grands modèles d'intelligence artificielle et des logiciels d'assistant de version hors ligne, qui ont été utilisés par les services de renseignement dans l'analyse des informations *top secret*. Ce qui est plus inquiétant, c'est l'extrême intérêt de Microsoft pour les informations personnelles de ses utilisateurs. Microsoft a dévoilé le 21 mai dernier sa nouvelle gamme de PC « Copilot + PC » et la fonctionnalité Recall, permettant au système d'exploitation de Windows d'enregistrer toutes les opérations de l'utilisateur pour que l'assistant d'intelligence artificielle puisse apprendre avec ces données. Microsoft a déclaré que cette fonctionnalité ne s'exécute que localement et que les données des utilisateurs ont été stockées cryptées. Cette déclaration n'a pourtant pas pu dissiper les doutes du public craignant un abus de cette fonctionnalité et une violation de données des utilisateurs. Face à la polémique, Microsoft a dû retarder le déploiement de Recall. Le 13 juin dernier, OpenAI, une entreprise investie par Microsoft, a embauché l'ancien directeur de la NSA, Paul Nakasone, comme membre du conseil d'administration. Les pratiques susmentionnées de Microsoft ont démontré clairement que la société, un partenaire important du programme de surveillance lié à la section 702, est de plus en plus influencée et manipulée par les services de renseignement américains. En retour, le gouvernement américain donne le feu vert aux pratiques monopolistiques de Microsoft qui consistent à promouvoir ses logiciels avec la mise à jour de Windows et d'Office.

Force est de mentionner l'incident du célèbre fournisseur antivirus américain CrowdStrike. Une mise à jour défectueuse de CrowdStrike a déclenché le 19 juillet dernier l'écran bleu de la mort sur des millions d'ordinateurs équipés du système d'exploitation Windows et a entraîné de grosses pertes aux secteurs, tels que les transports en commun et la santé, dans divers pays. Aucun acteur du secteur de cybersécurité ne souhaite voir un tel incident qui frappe notamment le secteur antivirus puisqu'il sapera considérablement à la

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

confiance des utilisateurs dans les logiciels antivirus tiers. Face à un incident aussi grave, la Cybersecurity and Infrastructure Security Agency (CISA), principal régulateur de cybersécurité des Etats-Unis, a adopté une indulgence poussée trop loin. Sans rien faire, la directrice de la CISA, Jen Easterly, a en revanche attribué cet incident à la « répétition » d'une attaque organisée par le groupe « Volt Typhoon », cherchant ainsi à détourner l'attention du public et à apporter du secours à Microsoft et à CrowdStrike. L'accident de CrowdStrike reflète l'énorme avantage des Etats-Unis dans la chaîne d'approvisionnement informatique. En tant que partenaires des services de renseignement américains, Microsoft et CrowdStrike sont naturellement mis à l'abri par le gouvernement américain. Au lieu d'être punies, ces deux entreprises continueront à élargir le marché international sous la protection du gouvernement et sous prétexte d'une « menace chinoise », et à fournir des informations de renseignement dans le cadre de la section 702.

En même temps, nous avons remarqué que de nombreux médias, personnalités et experts américains, européens, asiatiques et africains ont fait entendre la voix de la justice au sujet de « Volt Typhoon ». Un expert australien a publié un article intitulé « The geopolitics of cyber espionage »[13], indiquant que le rapport présenté par le gouvernement américain et Microsoft manque de preuves solides et que les services de renseignement américains ont inventé l'attaque de « Volt Typhoon » pour gagner le soutien du public et faire pression sur les décideurs de politiques, dans le but d'étendre encore leurs pouvoirs de surveillance sans mandat. Nous exprimons nos salutations respectueuses à ces personnalités étrangères qui parlent au nom de la justice.

V. Conclusion

Depuis des années, les agences du gouvernement fédéral américain, par intérêt égoïste, continuent de politiser le traçage de l'origine des cyberattaques. Pour plaire aux politiciens, aux agences du gouvernement et aux services de renseignement du pays, des entrerprises comme Microsoft et CrowdStrike ont baptisé les groupes de hackers de noms aux connotations géopolitiques évidentes tels que « Typhoon », « Panda » et « Dragon », tout en évitant les noms tels que « Anglo-Saxon », « Hurricane » ou « Koala », pour étaler leurs soi-disant « superbes » qualités technologiques et culturelles. En ignorant l'importance de la qualité du produit, elles finiront par créer une atmosphère nuisant au développement de l'industrie. Comme nous l'avons réitéré à plusieurs reprises dans nos rapports précédents, la Chine s'oppose toujours à la manipulation politique dans l'enquête sur des incidents de cybersécurité et à la politisation du traçage de l'origine des cyberattaques. Les services du gouvernement fédéral américain, qui jouent un rôle d'instigateur dans les coulisses, ont obtenu de gros budgets au Congrès grâce aux prétendues cyberattaques. Avec des ambitions de plus en plus démesurées, ces organisations vont finir un jour par se tirer une balle dans le pied. En quête d'intérêts illicites, des politiciens sans scrupules tels que Christopher Wray ont manipulé à plusieurs reprises le récit fallacieux concernant « Volt Typhoon » afin de duper le Congrès et le public américains. Ces politiciens vont sûrement être punis par la justice.

Aujourd'hui, alors que les conflits géopolitiques continuent de s'intensifier, l'industrie de la cybersécurité a plus que jamais besoin de bons échanges internationaux. Nous appelons une fois de plus à une vaste coopération internationale en matière de cybersécurité. Les entreprises et les établissements de

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

recherche du secteur devraient se concentrer sur les recherches techniques et offrir aux utilisateurs de meilleurs produits et services, pour que l'Internet puisse contribuer, de manière régulière et durable, au développement commun de la société humaine.

Centre national d'intervention d'urgence contre les virus informatiques
Laboratoire national d'ingénierie pour la technologie de prévention des virus informatiques
14 octobre 2024