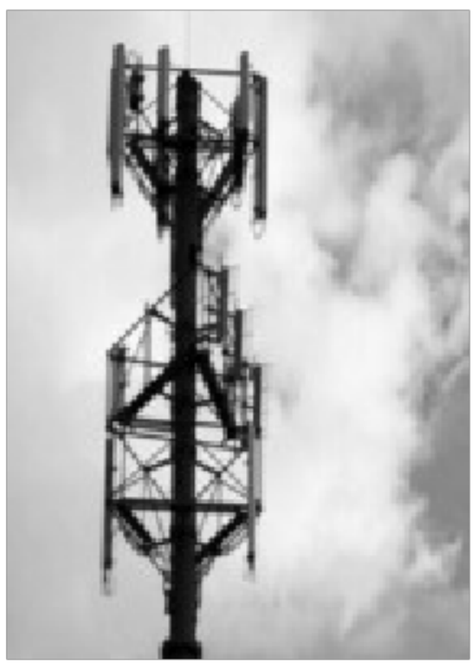
Contre les antennes relais et le réseau électrique



2 textes pratiques

Comment détruire des antennes-relais

Posté le 13 février 2020 sur attaque.noblogs.org :
https://attaque.noblogs.org/post/2020/02/17/tract-comment-detruire-des-antennes-relais/

Recette pour une antenne de téléphonie mobile de taille standard, utilisée par deux ou trois opérateurs de téléphonie.

D'habitude, sur le devant de l'installation il y a un panneau indiquant les entreprises qui l'exploitent.

Ingrédients :

- 2 ou 3 compas
- Des outils pour entrer (coupe-boulons, coupe-fils, etc.)
- Des gants, quelque chose pour couvrir son visage, des vêtements propres, un chapeau, une casquette ou un capuche (pour limiter les traces ADN)
- Du carburant (500 ml, du White spirit ou du kérosène, plutôt que de l'essence)
- Du carburant (100 ml d'essence)
- Des allume-feux, plusieurs briquets, une longue perche ou un bâton (allant jusqu'à 4,5 mètres)
- Des chiffons épais ou des torchons (pour absorber le carburant)
- Un petit pneu facile à transporter dans un sac à dos (pneu de brouette, de quad, de moto, etc.)

Étape 1.

Repérage de la cible. Trouvez le point faible de l'installation, c'est-à-dire l'endroit où les câbles du réseau partent du mât vertical et entrent à l'horizontale, ou presque, dans l'armoire électrique, qui est généralement un petit bâtiment en béton ou un coffret. Les câbles exposés peuvent être situés au niveau du sol ou jusqu'à 4,5 mètres de hauteur sur mât, par exemple. Notez les timing estimé, les points d'entrée et de sortie, où sont les caméras de

surveillance, les détecteurs de mouvement, l'éclairage, etc. Essayez d'exécuter l'action en 15 minutes.
Coincez bien le pneu entre les câbles et remplissez-le avec les chiffons, enroulez quelques chiffons autour des câbles qui montent au mât à partir de ce point. Trempez avec le carburant les chiffons à l'intérieur du pneu et ceux qui remontent le mât. Veillez à ne pas vous tacher de carburant, à éviter des preuves non nécessaires et qui pourraient être trouvées par la police scientifique et à ne pas vous brûler. Si vous utilisez un dispositif de retardement de la mise à feu, fabriqué en avance, placez-le à l'intérieur du pneu et enclenchez-le. Descendez.

Étape 2.

Si vous utilisez un dispositif de retardement, quittez immédiatement les lieux. Sinon, vérifiez rapidement le site et vos points de sortie. Cette deuxième vérification a pour but d'éviter toute détection, toute blessure inutile ou la mort à cause de la nature importante de l'action.

Étape 3.

Allumez le feu à l'aide d'un poteau ou d'un bâton enveloppé de chiffons imbibés de carburant. Ici, l'essence est préférable, car le vent peut devenir très fort là où ces mâts sont situés d'habitude. Allumez à distance les chiffons à l'intérieur du pneu, en vous éloignant le plus possible. Si le pneu est petit, le feu sera plus petit et la possibilité de détection est moindre. Entraînez-vous à opérer dans des environnements venteux, pour vous habituer à utiliser le feu en altitude et dans des circonstances difficiles. Partez immédiatement.

Sécurité

Débarrassez-vous de tout le matériel utilisé dans l'action de sabotage et ne revenez pas sur le lieu. Les équipes scientifiques de la police fouilleront minutieusement les environs de la cible, les points d'entrée et de sortie, ainsi que les itinéraires qui y mènent et qui en partent, à la recherche de toute trace qui pourrait être utilisé comme preuve.

Cette recette peut être adaptée et développée, afin d'être utilisée partout où elle est nécessaire ; des cibles et des systèmes plus grands et plus complexes nécessitent des plans d'attaque plus élaborés. On apprend des tentatives et des erreurs.

Contre la 5G et le monde qui en a besoin

Panne électrique – les impacts d’une attaque physique sur le réseau électrique

Posté le 31 mars 2020 sur Attaque.noblogs.org

“ Tout groupe terroriste qui souhaiterait mettre un pays à genoux a les moyens de le faire. ”

Grégoire Chambaz, Capitaine de l’armée suisse, au sujet des attaques sur le réseau électrique

Qu’ont en commun les aéroports, les installations de traitement de l’eau, les stations-service et les machines à espresso ? Une dépendance à l’égard d’un réseau fiable et stable de production et de distribution d’électricité. Dans le monde entier, nos réseaux électriques sont vieillissants, sur-sollicités, et de plus en plus exposés aux attaques. La centralisation et l’interdépendance accrue de ces réseaux signifient que le risque de défaillance à grande échelle n’a jamais été aussi grand. La prochaine fois que les lumières s’éteindront, elles pourraient ne plus jamais s’allumer.

Avant toute chose, imaginons ce que provoquerait une coupure de courant généralisée (un blackout). D’abord, les lumières, les vidéoprojecteurs et ordinateurs s’éteignent. Faute de pouvoir travailler ou étudier, vous cherchez donc à sortir. Il s’avère que la plupart des portes automatiques et portiques ne marchent plus, mais finalement vous parvenez à regagner la rue.

Vous souhaitez peut-être manger quelque chose. Cela dit, vous rencontrez plusieurs problèmes. Premièrement, si vous n’avez pas de monnaie, vous ne pouvez rien acheter, car la carte bancaire a besoin du réseau pour fonctionner. Au bout de quelques heures, l’ensemble des denrées qui étaient congelées dans les restaurants et supermarchés doivent être consommées ou jetées, ce qui entraine d’énormes pertes. Enfin, la plupart des plaques de cuisson étant électriques, vous devez probablement ressortir votre réchaud de camping pour pouvoir cuisiner.

Bien évidemment, les avions sont immédiatement cloués au sol faute de contrôle aérien. Les trains et transports publics (tram, métro) marchent à l'électricité, ils sont également à l'arrêt. La circulation terrestre est gênée, car les feux de circulation sont éteints, provoquant accidents et ralentissements. Cependant, cela ne dure pas bien longtemps : les pompes à essence fonctionnent aussi à l'électricité. Bientôt, les routes se vident.

Les échanges monétaires cessent, la bourse s'interrompt immédiatement. Sans informatique, sans communication, sans transport, la plupart des activités économiques s'arrêtent.

Vous suivez toutes ces informations avec attention. Puis vos téléphones, les antennes relais et les postes émetteurs n'ont plus d'énergie en stock. À partir de là, les nouvelles ne vous parviennent que de manière sporadique. Les décideurs aussi naviguent à vue : sans instruments de contrôle ou de communication centralisés, ils sont assez impuissants.

Le blackout : un super-risque

Vous l'aurez compris, l'électricité est critique. Elle est nécessaire pour tous les pans de notre activité, et nous ne savons plus vivre sans. Voici ce qu'explique Grégoire Chambaz :

> En quoi le risque de blackout est-il si singulier ? Avant tout, il s'agit d'un risque directement lié à un secteur critique, ce qui n'est pas le cas d'une pandémie ou d'une crise économique. Ce secteur critique, c'est l'approvisionnement en électricité. En effet, sans électricité, nos sociétés ne pourraient pas fonctionner. Si elles peuvent se permettre de se passer quelques jours de pétrole, une coupure de courant les affecte immédiatement.
>
> Comment cela se fait-il ? Pour deux raisons principales. La première, c'est que l'électricité irrigue tous les autres secteurs et infrastructures critiques. Ceux-ci sont pratiquement incapables de fonctionner sans elle. La deuxième raison, c'est que le blackout paralyse les deux secteurs critiques les plus importants après l'électricité, à savoir les télécommunications et les systèmes d'information. Sans eux, la coordination devient très difficile, surtout lors d'une situation de crise comme celle d'une coupure de courant. Cette centralité de l'électricité a été mise en évidence en 2010 dans un rapport de l'Office fédéral de la protection de la population (OFPP) sur la criticité des secteurs critiques. L'OFPP y définit la criticité comme « l'importance relative

d’un secteur critique en fonction des effets que son arrêt ou sa destruction auraient pour l’économie et la population ».

Dans ce cadre, le rapport effectue une évaluation qualitative (sur quatre degrés : 0, 1, 2, 3) de l’importance de chaque secteur critique par rapport aux autres. Les résultats font apparaître la centralité de l’approvisionnement électrique, touchant plus de secteurs que tout autre et provoquant le plus d’effets sur l’ensemble (voir tableau ci-dessous). Les systèmes d’information et les télécommunications passent respectivement en deuxième et troisième position. À l’inverse, les secteurs les plus vulnérables à l’arrêt des autres sont les services de secours et hôpitaux. En conséquence, la criticité de l’approvisionnement électrique détermine le blackout comme le risque plus important et motive sa qualification de « super-risque ».

“Le blackout, un « super-risque » : Une explication par la criticalité“, G. Chambaz, RMS No 05-2018 (cf. plus bas)

Recouvrement du réseau

Evaluation d’une sélection de secteurs critiques par l’OFPP. Chaque case indique la criticalité du secteur placé en ligne sur celui situé en colonne. Les numéros des cases renseignent de la force de cette criticalité (0 : pas criticalité, 4 : criticalité la plus forte). Le coefficient de criticalité indique l’importance relative d’un secteur pour l’ensemble. Le coefficient de dépen-dance signale la vulnérabilité relative d’un secteur par rapport à tous les autres.

Lire le tableau ↷	Approvisionnement électrique	Systèmes d'information etc.	Télécommunications	Transport routier	Systèmes automatisés etc.	Banques et services financiers	Internet	Approvisionnement pétrolier	Radiodiffusion et médias	Traitement des eaux usées	Transport ferroviaire	Approv. en eau potable	Produits pharmaceutiques	Services d'urgence	Transport aérien	Approvisionnement gazier	Hôpitaux et soins médicaux	Approv. alimentaire etc.	**Coefficient de criticalité**	**Nb de secteurs touchés**
Approvisonnement électrique		3	3	1	3	3	3	2	3	3	3	3	2	2	2	1	3	2	40	16
Systèmes d'information et réseaux	1		3	1	3	3	3	0	2	1	2	1	1	2	2	0	2	1	27	14
Télécommunications	2	2		1	3	3	3	1	2	0	1	0	0	3	2	1	2	0	26	13
Transport routier	1	1	1		1	0	0	2	2	1	1	1	2	3	1	1	1	2	19	14
Systèmes d'instrumentation et de surveillance	2	2	2	1		1	0	1	0	1	2	1	0	1	2	0	1	1	17	12
Banques et services financiers	2	1	2	0	0		1	2	1	0	1	0	0	1	1	1	1	3	14	11
Internet	0	2	2	0	2	2		0	2	0	1	0	0	1	1	0	1	1	14	9
Approvisionnement pétrolier	0	0	0	3	0	0	0		0	0	1	0	0	2	3	0	0	2	9	4
Radiodiffusion et médias	0	0	1	1	2	1	0	0		0	1	1	0	2	0	0	1	0	10	8
Traitement des eaux usées	0	0	1	0	0	1	0	0	1		1	1	0	1	1	0	2	0	9	8
Transport ferroviaire	0	0	0	0	0	0	0	2	1	0		0	1	0	1	0	0	2	5	4
Approvisionnement en eau potable	1	0	1	0	0	0	0	0	0	1	0		0	1	0	0	2	0	6	5
Produits pharmaceutiques	0	0	0	0	0	0	0	0	0	0	0	0		2	0	0	3	0	5	2
Services d'urgence	0	0	0	1	0	0	0	0	0	0	0	0	0		1	0	1	0	3	3
Transport aérien	0	0	0	0	0	0	0	0	1	0	0	0	1	0		0	0	1	2	2
Approvisionnement gazier	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0		0	0	1	1
Hôpitaux et soins médicaux	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0		0	1	1
Approvisionnement en denrées alimentaires	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		0	0
Coefficient de dépendance	9	11	16	10	14	14	10	10	15	7	14	8	7	22	17	4	20	15		
Nb de secteurs dépendants	6	6	9	8	6	7	4	6	9	5	10	6	5	13	11	4	12	9		

Quand tout le réseau électrique s’est effondré, redémarre-t-il en quelques instants ? Pas si simple. C’est une étape très délicate, parce que la demande doit être en permanence ajustée à l’offre, alors que les consommateurs veulent juste utiliser de l’électricité. Cette reconstruction se fait petit à petit, secteur par secteur, le tout sans télécommunication. Cela peut s’étaler sur des mois. Si le blackout ne dure qu’une journée, la récupération est rapide. S’il dure plus de 48 h, la récupération du réseau est moins probable, voire impossible. Tous les instruments qui pilotent les réseaux sont alimentés eux-mêmes en électricité, ils ont une autonomie de 2 à 5 jours. Une fois qu’ils n’ont plus de batterie, il faut se rendre sur place pour les redémarrer, de manière synchronisée avec le reste du réseau, toujours sans télécommunication. Si l’on n’a pas rétabli le réseau au bout de 5 jours, il ne pourra pas l’être sans aide extérieure. Si le blackout est régional, il y a des services d’urgence et de réparation qui peuvent être dépêchés. S’il est national ou continental, la situation peut perdurer voire même être fatale pour le réseau.

Ce scénario — catastrophique pour certains, rêvé pour d’autres —semble en tout cas irréaliste. Et pourtant… Ce réseau dont nous dépendons tant est loin d’être aussi solide qu’on pourrait le croire. Cela notamment à cause d’un élément : les transformateurs.

Les transformateurs, pièces centrales du réseau

On trouve des transformateurs à tous les niveaux du réseau. Le rôle d’un transformateur est simplement de modifier la tension de l’électricité. Certains l’augmentent pour qu’elle puisse circuler sur de longues distances (sur des lignes « haute tension »), d’autres la baissent afin qu’elle corresponde à la tension de nos prises de courant. Ils sont donc nécessaires pour raccorder les différentes pièces du réseau.

Il y a de très nombreux transformateurs, des petits, standardisés, qui se trouvent toutes les 3 à 4 maisons. En cas de défaillance, ceux-ci sont facilement remplacés. Et puis il y a ceux qui passent de la haute à la basse tension, qui sont énormes (et vieillissants). Ce sont ces derniers qui nous intéressent.

Ces choses sont monstrueuses, elles coûtent des millions d’euros, pèsent jusqu’à 350 tonnes. Elles font la taille de conteneurs d’expédition, entièrement constituées d’acier et de cuivre (métaux qui participent pour moitié au prix exorbitant du matériel). La fabrication de tels équipements est longue (5 à 20 mois), car ils sont élaborés sur mesure. En général, une seule pièce est

construite à la fois pour chaque modèle, il n’y a donc pas de pièces de rechange ni de pièces interchangeables. De ce fait, les réparations sont également très longues et complexes.

Leur transport est aussi un casse-tête. Le moyen le plus courant est le rail, mais seuls des wagons spécialisés peuvent supporter le poids. En France, c’est la STSI qui effectue ce genre de transport, elle dispose en tout de 10 wagons spéciaux. Aux États-Unis, ce sont seulement 30 wagons qui existent. Si le lieu n’est pas accessible en chemin de fer, le déplacement se fait par la route. On utilise alors des semi-remorques spécialisés, des « chenilles », dotés de 200 roues. Ils ont besoin d’autorisation pour traverser n’importe quelle municipalité, et il faut modifier la voirie et déplacer des lignes électriques pour permettre le passage. Bref, vous l’aurez compris, la construction comme le déplacement des transformateurs fait qu’ils ne sont pas facilement remplaçables.

Criticité des transformateurs

Nous l’avons dit, les transformateurs sont essentiels pour le réseau. Ils sont installés dans ce qu’on appelle des sous-stations, entourées de murs et de grillage. Certaines sous-stations sont très critiques. Lorsqu’un transformateur tombe en panne, cela peut avoir des effets en cascade sur l’ensemble du réseau. À titre d’exemple, il y a 55 000 sous-stations aux États-Unis. 350 d’entre elles sont les plus critiques. Des études réalisées par le gouvernement états-unien et des entreprises publiques estiment qu’à peine 9 sous-stations mises hors services pourraient faire tomber le réseau américain dans son ensemble pendant 18 mois. Souvenons-nous des conséquences d’un blackout de 5 jours. 18 mois seraient fatal pour le réseau.

Protection des transformateurs

Au vu de la criticité de tels équipements, on s’attendrait à ce qu’ils soient ultra-protégés. En réalité, la sécurité des postes est si déficiente qu’elle en est parfois comique.

Par exemple, une sous-station en Arizona — la sous-station Liberty — est une importante sous-station qui relie de nombreux états du Nord et du Sud sur le réseau occidental. Et en 2013, une série d’attaques physiques ont été menées contre cette station.

D’abord, quelqu’un a coupé les câbles de fibre optique de Liberty, ce qui a désactivé les communications pendant quelques heures. Ils n’ont jamais

compris qui avait réalisé cela, ni pour quelle raison. Mais deux semaines plus tard, de multiples alarmes ont commencé à se déclencher dans un centre de contrôle voisin, signalant que quelque chose n'allait pas à la sous-station. Ces alarmes se sont déclenchées pendant deux jours avant que quelqu'un ne soit envoyé pour vérifier. Quand ils sont arrivés, ils ont découvert que la clôture avait été ouverte, que le bâtiment de contrôle avait été cambriolé et qu'on avait utilisé plusieurs des ordinateurs sur place. Lorsque l'équipe de sécurité a vérifié les enregistrements des caméras, elle a réalisé que la plupart d'entre elles pointaient vers le ciel.

Ils ont donc installé de nouvelles caméras. Mais deux mois plus tard, une nouvelle effraction a eu lieu dans la même station. Lorsqu'ils ont vérifié les nouvelles caméras, ils ont découvert qu'aucune d'entre elles ne fonctionnait parce qu'elles n'avaient pas été programmées correctement. Si cet exemple vous a choqué, un autre exemple est encore plus frappant.

L'exemple de l'attaque Metcalf

En 2013 a eu lieu l'attaque la plus mystérieuse et intéressante du réseau électrique 6. Nous sommes donc à Coyote, en Californie, un peu en dehors de San Jose. À cet endroit, une entreprise appelée Metcalf possède une sous-station qui transmet une bonne partie de l'électricité de la Californie.

La nuit du 17 avril 2013, vers 1 heure du matin, quelqu'un s'introduit dans une chambre forte juste à côté de la sous-station et coupe des câbles de fibre optique. Il a fallu un peu de temps à l'opérateur pour s'en rendre compte. Dix minutes plus tard, une autre série de câbles est coupée dans une autre chambre forte à proximité.

30 minutes plus tard, une caméra de sécurité de la sous-station remarque une traînée de lumière au loin. Les enquêteurs comprendront plus tard que cette traînée de lumière était un signal lumineux effectué avec une lampe de poche. Immédiatement après – c'est-à-dire à 1 h 31 du matin — la caméra enregistre au loin le flash des fusils et les étincelles des balles frappant le grillage de la clôture. Toute cette action dans la caméra déclenche une alarme. Il est 1 h 37 du matin, quelques minutes après le début des tirs.

À 1 h 41, 10 minutes après le signal, le département du shérif reçoit un appel au 911 ; c'était en fait l'ingénieur de la centrale qui avait entendu les coups de feu. Le shérif alerté arrive 10 minutes plus tard, mais déjà, tout est calme. Il est arrivé une minute après qu'un autre signal de lampe de poche entraîne la fin de l'attaque.

Sur quoi tiraient les attaquants ? Justement, sur ces très gros transformateurs.

Les transformateurs sont en fait des choses physiquement simples, ce ne sont que des fils de cuivre enroulés dans de grosses cages métalliques. Mais les transformateurs chauffent, énormément, et sont donc refroidis. Pour ce faire, ils ont des réservoirs avec un liquide de refroidissement. Les tirs ont ciblé ces réservoirs de liquide, ils y ont fait des centaines de trous puis le liquide s'est échappé. La police est arrivée et n'a rien remarqué, il faisait sombre, on ne peut pas leur en vouloir. Plus de 200 000 litres d'huile se sont lentement écoulés. Après un petit moment, les transformateurs ont surchauffé et explosé. Un travailleur est arrivé quelques heures plus tard pour constater les dégâts, mais c'était déjà fait.

Cette attaque a alarmé les pouvoirs publics. Le FBI a enquêté. Ils ont trouvé des balles provenant de l'endroit où les attaquants avaient tiré, mais les empreintes digitales avaient été nettoyées. Ils ont trouvé des pierres marquant l'endroit où les attaquants devaient tirer, ce qui signifie qu'ils avaient déjà repéré ce site et savaient exactement où se présenter pour infliger un maximum de dégâts. Le fait d'avoir ciblé le réservoir de refroidissement montre qu'ils savaient quoi cibler pour générer des dégâts.

L’attaque a été qualifiée d’attaque terroriste sophistiquée, exécutée par une équipe de tireurs d’élite. On a pensé qu’elle pouvait être un essai pour une attaque plus importante sur le réseau électrique de la nation. Sauf que, selon le FBI, l’attaque n’était pas particulièrement difficile à réaliser, et elle aurait pu être réalisée par une personne seule, et cette personne n’était pas particulièrement précise dans ses tirs. « Nous ne pensons pas qu’il s’agissait d’une attaque sophistiquée », a déclaré John Lightfoot, qui gère les efforts de lutte contre le terrorisme du FBI dans la région de la Baie. « Il ne faut pas un très haut degré de formation ou d’accès à la technologie pour mener à bien cette attaque ». Quoi qu’il en soit, le FBI n’a aucune piste à ce jour.

17 des 21 transformateurs de la sous-station ont été mis hors service. Il en aurait suffi d’un ou deux supplémentaires pour mettre la Californie dans le noir. En l’occurrence, la compagnie d’électricité a pu rapidement contourner la sous-station. La Silicon Valley a continué à avoir de l’électricité, bien qu’on leur ait demandé de réduire leur consommation d’énergie pour la journée. Les dommages ont été réparés en 27 jours. Si plusieurs sous-stations avaient été touchées dans cette période, empêchant ainsi le re-routage, cela aurait pu être une toute autre histoire

Pour aller plus loin :

- L’article 3. Comment arrêter la société industrielle ? sur notre blog
- La vidéo de Grégoire Chambaz sur les black-out : “Le risque de blackout est-il réel ? “
- Le dossier spécial de la Revue Militaire Suisse : “Black out” (téléchargeable en pdf sur attaque.noblogs.org)*
- Le podcast de Ashes Ashes, en anglais : Episode 13 – Lights Out
- Un article sur le réseau européen est en préparation. Si vous avez des éléments intéressants à ce sujet (ou sur d’autres sujet d’ailleurs) n’hésitez pas à laisser un commentaire, ou contactez-nous sur les réseaux sociaux : www.facebook.com/vertresistance.

NdAtt. : cet article est issu du blog www.vert-resistance.org, reproduit ici sans demander rien à personne (mais avec des compliments pour le bon travail).

** Note d'Attaque : on remarquera que les militaires suisses ont pris en compte les effets qu'une épidémie pourrait avoir sur le réseau électrique de leur pays – à p. 39 (quatrième du fichier) on lit par exemple qu'à leur avis « Une pandémie peut grandement réduire le nombre d'employés du secteur électrique, ceux-ci étant malades, ou absents soit pour s'occuper de leurs proches, soit parce qu'ils craignent pour leur santé. Dans ces conditions, le réseau électrique pourrait ne plus suffisamment être encadré, un facteur de vulnérabilité pouvant mener à un blackout. »*