Lettre n°70 – Janvier 2018 - disponible sur omc.ceis.eu

TABLE DES MATIERES

LA REVISION DE L'ARRANGEMENT DE WASSENAAR DANS LE DOMAINE DES LOGICIELS D'INTRUSION ET SES CONSEQUENCES

Lors de la 23ème réunion plénière de l'Arrangement de Wassenaar qui s'est tenue les 6 et 7 décembre 2017 à Vienne, les États participants ont adopté des changements significatifs dans le régime de contrôle des biens et technologies en rapport avec les « logiciels d'intrusion ».

L'Arrangement de Wassenaar

Fondé en 1994, l'Arrangement de Wassenaar[1] est un régime multilatéral de contrôle des exportations, destiné à coordonner les politiques en matière d'exportations des armements conventionnels et des biens et technologies à double usage (usages civil et militaire) dans le but d'éviter le développement ou le renforcement de capacités militaires d'États ou de groupes terroristes qui pourrait nuire à la sécurité et à la stabilité régionales et internationales. Avec l'adhésion de l'Inde fin 2017, il regroupe désormais 42 États[2].

Du fait de la nature juridiquement informelle de l'Arrangement de Wassenaar, les États participants s'engagent politiquement à :

- Suivre les « directives », « éléments » et « meilleures pratiques » adoptés par l'Arrangement ;
- Contrôler, en vertu de leur législation nationale, les exportations de biens figurant sur la liste de l'Arrangement ;
- Rendre compte, par souci de transparence, des transferts d'armements conventionnels et de biens à double usage jugés sensibles, et des refus de transfert de biens à double usage en général ;
- Échanger des renseignements sur les exportations de biens et de technologies à double usage très sensibles.

Depuis 2000, les dispositions de l'Arrangement s'imposent à tous les États membres de l'Union européenne. Elles sont en effet reprises, avec les dispositions d'autres accords internationaux, dans un règlement de l'UE régulièrement actualisé, actuellement le règlement (CE) n° 428/2009 du 5 mai 2009[3].

[1] http://www.wassenaar.org/about-us/

[2] Afrique du Sud, Allemagne, Argentine, Australie, Autriche, Belgique, Bulgarie, Canada, Corée, Croatie, Danemark, Espagne, Estonie, Etats-Unis, Finlande, Grèce France, Hongrie, Inde, Irlande, Italie, Japon, Lettonie, Lituanie, Luxembourg, Malte, Mexique, Norvège, Nouvelle-Zélande, Pays-Bas, Pologne, Portugal, République tchèque, Roumanie, Royaume-Uni, Russie, Slovaquie, Slovénie, Suède, Suisse, Turquie et Ukraine.

[3] Règlement (CE) n° 428/2009 du Conseil du 5 mai 2009 instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et du transit de biens à double usage (http://eur-lex.europa.eu/legal-content/FR/ALL/?uri=celex:32009R0428)

Les biens et technologies numériques et les « logiciels d'intrusion »

Les biens et technologies numériques sont principalement traités dans la liste des biens à double usage (BDU)[4] : catégories 4 (calculateurs et matériels connexes, dont les logiciels assurant des fonctions de télécommunications ou de réseaux locaux) et 5 (partie 1, « télécommunications », et partie 2, « sécurité de l'information »).

Dès la première version, l'Arrangement a pris en compte certains biens et technologies numériques, en particulier les calculateurs et autres outils de cryptographie et de cryptanalyse, alors considérés quasiment comme du matériel de guerre. La liste a évolué avec les années pour tenir compte du développement des technologies numériques et de l'évolution de leur sensibilité. Ainsi, en 2012 et 2013, elle a intégré divers biens (systèmes, équipements, composants, logiciels) et technologies[5] pouvant servir au fonctionnement des « logiciels d'intrusion ». Ces derniers font quant à eux seulement l'objet d'une définition et ne sont pas inclus en tant que tel dans la liste[6].

L'intégration avait pour objectif de limiter la prolifération des « logiciels d'intrusion » qui permettent notamment l'interception des télécommunications mobiles, la surveillance des réseaux IP et l'accès non autorisé à des systèmes informatiques. Cependant, la formulation retenue s'est révélée inadaptée aux évolutions des technologies numériques et a suscité de vives critiques de la part des entreprises et des chercheurs en cybersécurité. Ces derniers dénonçaient l'imprécision des termes retenus par l'Arrangement et les restrictions qu'elle pouvait impliquer pour les entreprises de sécurité qui exportent des solutions de cybersécurité ou pour les échanges d'information entre les chercheurs, notamment dans un contexte de cyberattaques d'envergure internationale[7].

En 2016, suites à ces réactions, les États-Unis ont proposé une révision des dispositions relatives aux « logiciels d'intrusion », sans toutefois parvenir à un consensus. Finalement, une révision a été adoptée lors de la réunion plénière de décembre 2017.

---

[4] http://www.wassenaar.org/wp-content/uploads/2018/01/WA-DOC-17-PUB-006-Public-Docs-Vol.II-2017-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf

[5] Dans l'Arrangement, le terme « technologie » désigne les « *connaissances spécifiques requises pour le « développement », la « production » ou l'« utilisation » d'un produit ; ces connaissances se transmettent par la voie de la 'documentation technique' ou de l''assistance technique'* ».

[6] Dans l'Arrangement, le « logiciel d'intrusion » est seulement définit de la façon suivante : « *logiciel spécialement conçu ou modifié pour éviter la détection par un «outil de surveillance», ou pour tromper les «contre-mesures de protection» d'un ordinateur ou d'un dispositif en réseau, et pour effectuer les tâches suivantes: a. extraction de données ou d'informations à partir d'un ordinateur ou d'un dispositif de réseau, ou modification des données système ou utilisateur; ou b. modification du chemin d'exécution standard d'un programme ou d'un processus afin de permettre l'exécution d'instructions provenant de l'extérieur* ». Toutefois, il « *n'inclut aucun des éléments suivants : a. hyperviseurs, programmes de débogage ou outils de rétro-ingénierie de logiciels (SRE) ; b. « logiciel » de gestion des droits numériques (GDN) ; ou c. « logiciel » conçu pour une installation par les fabricants, les administrateurs ou les utilisateurs, à des fins de suivi ou de récupération des actifs. 2. Les dispositifs en réseau incluent les dispositifs mobiles et les compteurs intelligents* ».

[7] https://www.scmagazineuk.com/wassenaar-arrangement-inhibits-international-cyber-security-efforts/article/530845/

Ainsi, quels sont les changements opérés par la révision de 2017 et quelles peuvent en être les conséquences ?

Les changements de la révision de 2017

Afin notamment d'adapter les dispositions de la liste BDU relatives aux « logiciels d'intrusion » aux besoins de la cybersécurité, les États participants ont adopté trois changements[8] :

- Le remplacement de termes utilisés pour désigner les biens concernés par le contrôle ;
- L'ajout d'une exception relative aux logiciels de mise à jour ou de mise à niveau ;
- L'ajout d'exemptions pour le contrôle des technologies pouvant servir au développement des « logiciels d'intrusion ».

La nouvelle rédaction des dispositions relatives aux biens

Jusqu'à la révision de 2017, les biens relatifs aux « logiciels d'intrusion » entrant dans le régime de contrôle de l'Arrangement étaient désignés de la manière suivante dans la liste BDU : les systèmes, équipements et composants ainsi que les logiciels spécialement conçus ou modifiés pour la génération, l'exploitation ou la livraison de « logiciels d'intrusion », ou pour la communication avec ceux-ci[9]. Cette formulation a rapidement montré que les termes employés pouvaient être interprétés plus ou moins largement et porter préjudice à des entreprises ou des chercheurs en cybersécurité, notamment par des interprétations différentes des divers États participants.

Ainsi, les États participants ont décidé d'adopter une nouvelle rédaction de ces dispositions. Les termes anglais « *operation* » et « *communication with* » ont été remplacé par les termes « *command and control* »[10]. Les nouvelles dispositions ne désignent donc plus les biens permettant « d'exploiter » ou de « communiquer avec » un « logiciel d'intrusion » mais les biens qui permettent de donner des ordres et de faire exécuter des actions à un « logiciel d'intrusion ».

Cette nouvelle rédaction diffère sensiblement de la précédente en ce qu'elle adopte une approche différente. Elle fait référence à la finalité du bien qui interagit avec le « logiciel d'intrusion », contrairement à la rédaction précédente qui portait sur la capacité des biens concernés.

Notons enfin que l'expression « *command and control* » correspond bien à la terminologie employée dans le domaine des cyberattaques[11].

---

[8] https://www.lawfareblog.com/wassenaar-export-controls-surveillance-tools-new-exemptions-vulnerability-research

[9] Dispositions 4. A. 5. et 4. D. 4. de la liste BDU antérieures à 2017 : http://www.wassenaar.org/wp-content/uploads/2016/04/WA-LIST-15-1-CORR-1-2015-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf

[10] Dispositions 4. A. 5. et 4. D. 4. de la liste BDU issues de la revision de 2017 : http://www.wassenaar.org/wp-content/uploads/2018/01/WA-DOC-17-PUB-006-Public-Docs-Vol.II-2017-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf

[11] https://www.trendmicro.com/vinfo/us/security/definition/command-and-control-(c-c)-server

L'exception relative aux logiciels de mise à jour ou de mise à niveau

La révision de 2017 a introduit une exception spécifique au contrôle de l'exportation des logiciels pouvant servir au fonctionnement des « logiciels d'intrusion ». Désormais, les logiciels spécialement conçus et limités à fournir des mises à jour ou des mises à niveau « logicielles » n'entrent plus dans le régime de contrôle de la liste BDU lorsqu'ils répondent aux conditions suivantes[12] :

- Lorsque la mise à jour ou la mise à niveau ne peut s'exécuter qu'avec l'autorisation du propriétaire ou l'administrateur du système ; et
- Lorsque le logiciel mis à jour ou mis à niveau ne constitue pas :
    - Un logiciel permettant la génération, le commandement et le contrôle ou la livraison d'un « logiciel d'intrusion » ; ou
    - Un « logiciel d'intrusion ».

Les exemptions au contrôle des technologies pouvant servir au développement des « logiciels d'intrusion »

Afin d'éviter le risque d'un contrôle excessif sur les recherches et la coopération internationale en matière de cybersécurité, la révision de 2017 ajoute deux exemptions pour le contrôle des technologies pouvant servir au développement des logiciels qui permettent la génération, le commandement et le contrôle ou la livraison des « logiciels d'intrusion » ou au développement de ces derniers[13] :

- Pour ce qui concerne la « divulgation de vulnérabilité » ;
- Pour ce qui concerne la « réponse aux cyber-incidents ».

Dans l'Arrangement de Wassenaar, la « divulgation de vulnérabilité » désigne le fait d'identifier, de notifier ou de communiquer une vulnérabilité aux personnes ou aux organisations chargées de conduire ou de coordonner la correction de la vulnérabilité. Elle désigne également le fait d'analyser une vulnérabilité en collaboration avec les personnes et organisations précédemment mentionnées[14].

S'agissant de la « réponse aux cyber-incidents », elle désigne le fait d'échanger les informations nécessaires sur un incident de cybersécurité avec les personnes ou les organisations chargées de conduire ou de coordonner les mesures pour remédier à l'incident[15].

Enfin, si les échanges d'information sur les vulnérabilités et les cyber-incidents ne font plus obligatoirement l'objet d'un contrôle, les autorités des États participants disposent toujours du droit de vérifier la conformité des échanges d'information avec les dispositions relatives aux technologies impliquées dans les « logiciels d'intrusion »[16].

---

[12] Note relative à la disposition 4. D. 4.

[13] Dispositions 4. E. 1. a. et c.

[14] Note technique numéro 1 de la Note 1 de la disposition 4. E. 1. c.

[15] Note technique numéro 2 de la Note 1 de la disposition 4. E. 1. c.

[16] Note 2 de la disposition 4. E. 1. c. de liste BDU

Tableau récapitulatif des changements opérés par la révision de 2017

Dispositions	Version antérieure à la révision de 2017	Version issue de la révision de 2017
Dispositions relatives aux biens	4. A. 5. Systèmes, équipements et composants spécialement conçus ou modifiés pour la génération, l'exploitation ou la livraison de « logiciels d'intrusion », ou pour la communication avec ceux-ci. 4. D. 4. « Logiciels » spécialement conçus ou modifiés pour la génération, l'exploitation ou la livraison de « logiciels d'intrusion », ou pour la communication avec ceux-ci.	4. A. 5. Systèmes, équipements et composants spécialement conçus ou modifiés pour la génération, **le commandement et le contrôle** ou la livraison de « logiciels d'intrusion ». 4. D. 4. « Logiciels » spécialement conçus ou modifiés pour la génération, **le commandement et le contrôle** ou la livraison de « logiciels d'intrusion ». ***Note 4. D. 4 ne s'applique pas aux « logiciels » spécialement conçus et limités à fournir des mises à jour ou des mises à niveau « logicielles » répondant aux conditions suivantes :*** ***a. La mise à jour ou la mise à niveau ne fonctionne qu'avec l'autorisation du propriétaire ou de l'administrateur du système qui le reçoit ; et*** ***b. Après la mise à jour ou la mise à niveau, le « logiciel » mis à jour ou mis à niveau n'est pas l'un des éléments suivants :*** ***1. « Logiciel » spécifié par 4. D. 4. ; ou*** ***2. « Logiciel d'intrusion ».***
Dispositions relatives aux technologies	4. E. 1. a. « Technologie », au sens de la note générale relative à la technologie, pour le « développement », la « production » ou l' « utilisation » des équipements ou « logiciels » visés dans les sous-catégories 4A ou 4D.	4. E. 1. a. « Technologie », au sens de la note générale relative à la technologie, pour le « développement », la « production » ou l' « utilisation » des équipements ou « logiciels » visés dans les sous-catégories 4A ou 4D.

	c. « Technologie » pour le « développement » de « logiciels d'intrusion ».	c. « Technologie » pour le « développement » de « logiciels d'intrusion ». ***Note 1 4. E. 1. a. et 4. E. 1. c. ne s'appliquent pas à la "divulgation de vulnérabilités" ou aux "réponses aux cyber-incidents".*** ***Note 2 La note 1 ne diminue pas le droit des autorités nationales de vérifier la conformité aux dispositions 4. E. 1. a. et 4. E. 1. c.*** ***Notes techniques*** ***1. "Divulgation de vulnérabilités", processus d'identification, de déclaration ou de communication d'une vulnérabilité à, ou analyser une vulnérabilité avec, les individus ou les organisations chargés de diriger ou de coordonner correction dans le but de résoudre la vulnérabilité.*** ***2. « Réponse aux incidents cybernétiques », processus d'échange nécessaire des informations sur un incident de cybersécurité avec des individus ou des organisations responsables de la conduite ou de la coordination des mesures correctives pour l'incident de cybersécurité.***

Les conséquences de la révision de 2017

La conséquence principale de la révision de 2017 est l'assouplissement du régime de contrôle des exportations des biens et technologies impliqués dans les logiciels d'intrusion. A ce titre, la révision devrait profiter à l'écosystème de la cybersécurité. Par ailleurs, elle devrait relancer les débats sur les projets législatifs nationaux et européen qui sont en cours et sur l'avenir du régime de contrôle des « logiciels d'intrusion ».

L'écosystème de la cybersécurité

Les nouvelles dispositions issues de la révision de 2017 devraient répondre aux attentes de l'évolution de l'écosystème de la cybersécurité. En effet, l'imprécision des anciennes dispositions conduisaient à restreindre le développement de nouveaux programmes de cybersécurité tels que la recherche et la correction de vulnérabilités (les programmes de Bug Bounty notamment)[17].

L'assouplissement du régime de contrôle devrait ainsi faciliter le développement de ces programmes et les échanges d'informations entre les acteurs privés de la cybersécurité. Par ailleurs, la révision de 2017 devrait également assurer une meilleure protection contre les risques d'ingérence des États dans les recherches de

[17] https://threatpost.com/bug-bounties-in-crosshairs-of-proposed-us-wassenaar-rules/113204/

vulnérabilités[18]. Ces derniers pouvaient en effet accéder à des informations sur les recherches en cybersécurité lors de la délivrance d'une licence d'exportation.

Soulignons cependant que si l'écosystème de la cybersécurité se réjouit des nouvelles dispositions de l'Arrangement de Wassenaar, des zones d'ombre demeurent sur les définitions retenues dans l'Arrangement selon certaines entreprises et des chercheurs en cybersécurité[19]. En particulier, la définition large relative aux « logiciels d'intrusion » peut avoir pour inconvénient d'inclure des outils de cybersécurité légitimes autres que ceux portant sur la divulgation de vulnérabilités ou sur la réponse aux cyber-incidents[20].

Les réformes législatives relatives au contrôle des biens et technologies à double usage

La révision de 2017 devrait particulièrement impacter les projets européen et israélien de réforme de leur législation sur le contrôle des biens et technologies à double usage.

Ainsi, l'Union européenne souhaite réformer son régime de contrôle notamment en ce qui concerne les « logiciels d'intrusion ». D'une part, le projet vise à inclure la protection des droits de l'homme dans le régime de contrôle et, d'autre part, à adapter le contrôle aux exportations de solutions de cybersécurité[21].

Bien que n'étant pas partie à l'Arrangement de Wassenaar, Israël a, de son côté, retranscrit dans sa législation les dispositions relatives aux « logiciels d'intrusion » en y ajoutant toutefois de nombreuses précisions[22]. Comme l'Union européenne, Israël souhaite aujourd'hui réformer sa législation pour ne pas pénaliser les entreprises de cybersécurité[23].

Les nouvelles dispositions de l'Arrangement de Wassenaar devraient donc s'insérer dans les débats sur ces projets de réforme. L'Union européenne et Israël ne devraient normalement pas remettre en question la révision de 2017 mais ils pourraient néanmoins ajouter des précisions supplémentaires à ces nouvelles dispositions.

Évolution à venir du régime de contrôle des « logiciels d'intrusion »

Si la révision de 2017 a permis d'assouplir le régime de contrôle des biens et technologies en rapport avec les « logiciels d'intrusion » et de l'adapter ainsi aux besoins de la cybersécurité, l'année 2018 devrait voir se tenir de nombreuses discussions sur l'avenir de ce régime

En effet, le département du commerce américain et les entreprises américaines de cybersécurité, qui étaient à l'initiative de la révision de 2017, devraient proposer de nouvelles exceptions ou exemptions[24], voire des changements substantiels plus importants, par exemple une révision de la définition des "logiciels d'intrusion".

---

[18] https://www.the-parallax.com/2017/12/27/2017-cybersecurity-privacy-news-review/

[19] https://www.cyberscoop.com/wassenaar-arrangement-cybersecurity-katie-moussouris/

[20] https://www.lawfareblog.com/wassenaar-export-controls-surveillance-tools-new-exemptions-vulnerability-research

[21] https://www.marietjeschaake.eu/en/european-parliament-adopts-position-on-export-control-reform

[22] https://www.lawfareblog.com/can-export-controls-tame-cyber-technology-israeli-approach

[23] https://www.defensenews.com/home/2016/06/20/israel-liberalizes-cyber-export-policy/

[24] https://www.lawfareblog.com/wassenaar-export-controls-surveillance-tools-new-exemptions-vulnerability-research

D'autres États, comme l'Inde, pourraient être également favorables à un assouplissement du régime de contrôle afin de pouvoir développer leur capacité de cyberdéfense[25].

Ces positions devraient toutefois se heurter aux défenseurs des droits fondamentaux et des libertés sur internet, qui seront attentifs voire hostiles à toute volonté d'assouplissement.

[25] http://www.thehindubusinessline.com/opinion/the-wassenaar-effect/article7612180.ece

LES CYBERMENACES POUVANT AFFECTER L'APPROVISIONNEMENT EN ELECTRICITE

L'approvisionnement en électricité est d'importance vitale pour un pays. L'ensemble d'une population et des rouages socio-économiques peut soudainement se retrouver privé de tout ce qui leur permet de fonctionner. **S'attaquer au réseau électrique, c'est mettre à l'arrêt toute une société, engageant parfois la vie des individus.** D'après la société de cybersécurité Symantec[26], le groupe de hackers Dragonfly a commencé dès 2013 à prendre le contrôle des systèmes informatiques des grands opérateurs d'énergie de plusieurs pays occidentaux, mettant en place des outils d'espionnage tout en se donnant la possibilité de lancer à tout moment des opérations de sabotage. En décembre 2015, plusieurs entreprises d'approvisionnement en électricité ukrainiennes sont ainsi affectées par des malwares spécifiques, provoquant des black-out sur une partie du pays. A Noël 2016, le réseau électrique de Kiev est interrompu pendant une heure, quelques temps après la découverte d'un malware dans un ordinateur du distributeur municipal d'électricité de la ville de Burlington (USA). En mai dernier, des centrales électriques américaines et britanniques sont la cible de nombreuses tentatives d'intrusions. Enfin, les chercheurs et les sociétés de cybersécurité trouvent très régulièrement de nouveaux malwares spécifiquement destinés aux attaques contre les systèmes de contrôle industriel (ICS) très largement utilisés dans les secteurs de l'énergie.

L'actualité ne tarit pas. Au regard de ces précédents, on peut craindre une probabilité forte d'occurrence d'attaques ciblant les fournisseurs d'électricité. Leurs systèmes de contrôle industriel, et plus particulièrement les SCADA (système de supervision et d'acquisition de données / *Supervisory Control and Data Acquisition)*, sont très vulnérables aux attaques extérieures, notamment aux *Advanced Persistant Threat* (APT). Ce type d'attaque nécessite une grande expertise, une longue préparation en amont et un degré élevé de dissimulation. L'objectif est de pouvoir installer des codes malveillants sur un système d'information et de le maintenir durant une longue période, dans le but d'espionner le système de l'organisme, d'en prendre le contrôle à distance et, au moment choisi, de le rendre inopérant, dans le cas précis, en coupant la fourniture d'électricité. La particularité de ce type d'attaque réside dans l'extrême difficulté à le détecter et à l'anticiper. De plus, les cybercriminels ne cessent de s'adapter à l'environnement de la cible et aux évolutions technologiques des systèmes d'information.

La présente note a pour objectif présenter les principales caractéristiques de ces cyberattaques ainsi que les différentes étapes de la KillChain[27] qui peuvent mener jusqu'à une coupure de la production ou de la distribution d'électricité dans de vastes zones. Elle rappelle ensuite les principales mesures qui peuvent être mises en place par les États et par les opérateurs pour limiter les risques de cyberattaques sur les systèmes électriques.

---

[26] *https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf.*

[27] *Telle que définie par Lockheed Martin. Voir le schéma en annexe.*

Les grandes caractéristiques de ces attaques

Les mobiles et les profils potentiels des attaquants

Priver d'électricité un territoire, voire un pays entier pourrait être un objectif de tout hacker malveillant, qu'il cherche simplement à montrer ses talents, à manifester son mécontentement (ce serait le cas d'un ancien employé voulant se venger par exemple), ou son opposition politique, religieuse ou sociale (ce qui est le principe de l'hacktivisme), à gagner de l'argent (une rançon pouvant être demandée pour cesser l'attaque), ou encore à s'attaquer à la vie économique, sociale et politique d'un pays pour le déstabiliser et lui imposer des conditions (dans un objectif politico-militaire) ou pour semer la terreur (dans un objectif terroriste). Mais une attaque d'ampleur contre les systèmes de production ou de distribution d'électricité nécessite une expertise profonde dans les technologies d'APT, des outils spécifiques permettant de mener l'attaque, les moyens opérationnels de commander les divers malwares injectés, et beaucoup de temps. **Il ne peut donc s'agir ni d'une attaque opportuniste, ni d'une équipe d'attaquants débutants.** Ces attaques seront a priori toujours le fait d'États, ou de groupes cybercriminels puissants plus ou moins inféodés à des États.

L'effet principal recherché par les attaquants est la paralysie, voire la dévastation d'un pays : le scénario de black-out.

- **Dans un objectif terroriste :**
  Les terroristes ont aujourd'hui davantage privilégié des actions contre les individus. Cependant, il est probable qu'une attaque cyber de plus grande ampleur soit menée un jour contre un pays, dans le but d'imposer une idéologie par la soumission et par la peur. Des mafias ou des organisations criminelles transnationales peuvent également avoir un intérêt à déstabiliser un Etat dans une entreprise de sabotage à grande échelle.
- **A dessein hacktiviste** :
  Des militants peuvent porter atteinte à l'image d'un Etat, d'une entreprise fournissant l'électricité, dans un but malveillant. L'émergence d'un tel mobile et le regroupement d'une équipe engagée dans une cause pourraient aboutir à l'implémentation d'une APT. En 2012, un membre du collectif Anonymous a publié une liste des systèmes SCADA Israéliens (identifiants de connexion, listes d'URL en équivalent IP, …).
- **Pour une finalité géopolitique :**
  Le contexte géopolitique est très important dans la détermination du mobile des attaquants. Chaque pays détient ses propres intérêts stratégiques et ses propres relations diplomatiques. Il est donc difficile d'établir une règle à ce sujet. De manière générale, les attaquants peuvent provenir d'Etats concurrents ou d'agences gouvernementales ayant un intérêt à déstabiliser l'Etat cible, pour des raisons économiques, financières ou politiques ou en complément à d'autres actions, diplomatiques ou militaires par exemple. Dans un même esprit que l'équilibre stratégique de la dissuasion nucléaire qui perdure depuis un demi-siècle, une attaque cyber sur un autre Etat peut aussi être un moyen d'exposer sa force et d'intimider son ennemi.

La probabilité que des hackers provoquent la coupure d'électricité (stade ultime d'une attaque longuement préparée en amont) est plus élevée lors de grands évènements culturels ou de périodes symboliques. Cela renforce en effet l'impact médiatique et social de l'attaque. Par ailleurs, l'impact technique, et donc aussi médiatique et social, sera amplifié en choisissant de provoquer la coupure d'électricité à des moments où la reprise d'activité sera la plus longue et difficile à conduire (fin de journée, fin de semaine, périodes de fêtes, grand évènement monopolisant l'attention des techniciens et des décideurs). C'est ainsi que les cyberattaques qui ont affecté le réseau électrique ukrainien en 2015 et en 2016 ont eu lieu fin

décembre, en pleine préparation des fêtes de Noël en 2016. Le risque est de même particulièrement élevé lors des évènements d'ampleur mondiale, tels que les Coupes du Monde ou les sommets réunissant plusieurs chefs d'Etat.

La complexité de ces attaques et les opportunités

Une attaque visant à provoquer un black-out électrique est très complexe à mettre en œuvre et nécessite **une longue préparation en amont et de nombreux moyens techniques, humains et financiers pour avoir l'effet escompté, c'est-à-dire la réussite ou du moins, un risque faible d'échec.** La sélection de la cible est également d'une importance fondamentale et nécessitera que les pirates informatiques effectuent une reconnaissance préalable de « l'environnement » du système.

Cela étant, les ICS/SCADA sont des systèmes informatiques très sophistiqués, donc très vulnérables. La multiplicité des failles de ces systèmes en fait des cibles de choix pour des hackers aguerris. Leur architecture est complexe, constituée de multiples systèmes d'exploitation interconnectés et hétérogènes, de nombreuses interfaces et d'objets connectés (IOT), rendant parfois impossible de protéger les parties les plus sensibles par du cloisonnement. De plus, leurs mises à jour de sécurité sont le plus souvent difficiles à appliquer, faute de pouvoir interrompre la chaîne de production. Certains SCADA ont de plus été conçus il y a plusieurs décennies, lorsque les systèmes industriels n'étaient pas connectés à internet, et les protocoles de sécurité n'ont pas été adaptés depuis. Les failles à exploiter sont donc nombreuses, constituant une opportunité pour les attaquants.

Les difficultés d'attribution de l'attaque

L'attribution certaine des attaques reste un problème non résolu dans la majeure partie des cas. Il est toutefois possible qu'elle soit revendiquée par les attaquants eux-mêmes. C'est souvent le cas des hacktivistes qui cherchent ainsi un retentissement médiatique, vecteur de transmission de leur idéologie. Il peut aussi arriver que les attaquants utilisent le modus operandi d'autres groupes cybercriminels dans le but de brouiller les pistes quant à l'origine de la malveillance, voire même de leur faire attribuer l'attaque (*copycat*). Le commanditaire d'une attaque est plus difficile encore à connaître avec certitude. Les Etats commanditaires confient souvent leurs actions offensives à des groupes de hackers constitués, en échange d'avantages financiers ou en tolérant leurs actions cybercriminelles sous réserve qu'elles n'affectent pas l'Etat considéré, ou en recrutant ponctuellement des *mercenaires nationaux ou étrangers*[28].

L'objectif du processus de recrutement est de constituer une équipe qui aura toutes les compétences attendues pour mener l'attaque à ses différents stades. Une équipe de pirates va se constituer sur la base d'un intérêt commun (une cause à soutenir, un ennemi partagé, une ferveur idéologique ou nihiliste). Le

[28] *L'Etat peut également utiliser des stratagèmes afin de faire croire au hacker qu'il est recruté par les forces armées de son propre Etat, pour une cause nationaliste. Il va « tutorer » l'équipe de hackers et évaluer ses capacités opérationnelles à mener l'attaque, assurer la fourniture des outils nécessaires et des moyens financiers. Lorsque la confiance sera établie, l'Etat partagera ses connaissances stratégiques sur la cible.*

processus de recrutement doit être mené en toute discrétion, c'est la raison pour laquelle les forums du DarkNet sont un canal de communication intéressant pour les hackers[29].

Les grandes étapes et les caractéristiques d'une attaque : la *Kill Chain*

Qu'elle ait pour objectif final de l'espionner ou d'affecter fortement son fonctionnement, la prise de contrôle d'un système d'information complexe, comme ceux mis en œuvre dans le secteur de l'énergie, nécessite une série d'actions allant de la reconnaissance de l'environnement de la cible jusqu'à la mise en place de la "charge utile" à l'endroit voulu et à son exploitation. Ces différentes actions sont reparties en grandes étapes, regroupées par Lockheed Martin sous l'appellation de "*Cyber Kill Chain*" (voir le schéma en annexe).

Toutes ces actions doivent impérativement se faire dans la plus grande discrétion et de la manière la plus furtive possible pour ne pas alerter les administrateurs et les usagers du système et éviter la détection des malwares par les dispositifs de sécurité ou en cas d'audit technique du système.

La compréhension de ces différentes étapes est essentielle pour mettre en place les mesures de protection et de défense des systèmes pouvant être la cible de telles attaques.

A titre d'illustration, le schéma ci-dessous présente l'application de la *Kill Chain* lors de l'attaque contre les fournisseurs d'électricité ukrainiens en décembre 2015.

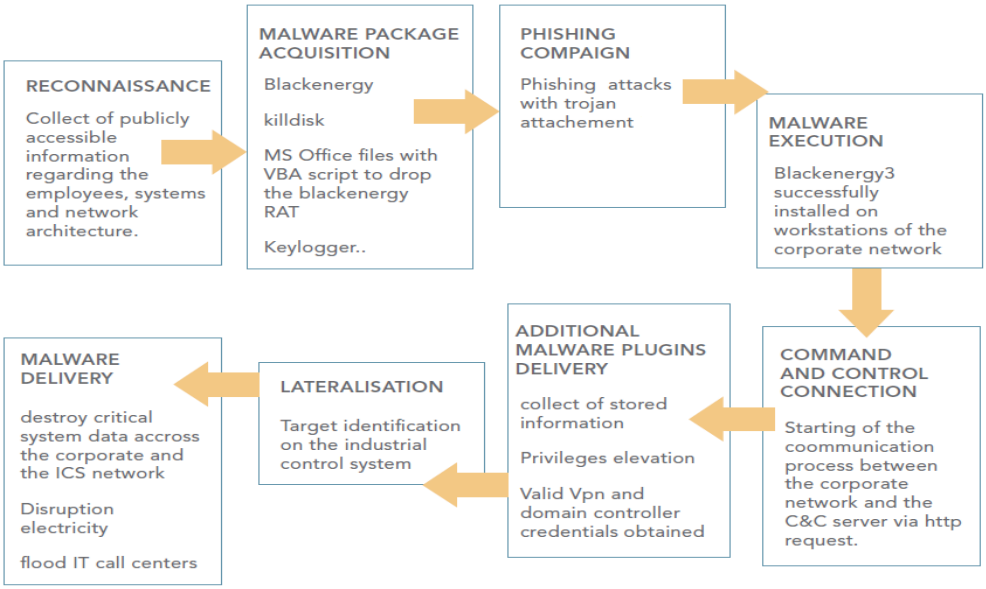


Schéma descriptif du mode opératoire des attaquants des fournisseurs d'électricité ukrainiens en 2015.

Etape 1 : la reconnaissance de l'environnement de la cible

Les attaquants vont chercher le plus d'informations possibles sur le système cible, de nature technique, humaine et organisationnelle, afin d'avoir la meilleure compréhension possible de son

[29] *Ce qui a été le cas pour l'attaque de 2015 contre l'Ukraine : des appels à la constitution d'équipes et des recherches d'exploits spécifiques à un type de SCADA ont été effectué sur les forums du DarkNet quelques années avant.*

architecture, de ses composants, de ses usagers, et in fine, des vulnérabilités pouvant être exploitées pour s'introduire dans le système et conduire les actions ultérieures.

Ces informations pourront être obtenues par des voies très diverses : investigations techniques plus ou moins licites, à distance via internet, sur les systèmes d'information de l'entreprise ou de ses correspondants (clients, sous-traitants …), social engineering sur le personnel (informations publiées sur les réseaux sociaux, espionnage des moyens de communication personnels de personnes clefs …), sources ouvertes diverses, notamment les sites Web de l'entreprise et de ses fournisseurs, interception de mails, informateurs ayant accès à l'entreprise, etc.

Cette recherche pourra porter notamment sur les points suivants :

- **Technique :** processus industriels mis en œuvre, architecture générale du réseau et des systèmes reliés, équipements en place (fournisseurs, modèles, versions logicielles, situation des patchs de sécurité …), nature et efficacité des portes d'accès (ports ouverts, accès distants des employés et des sous-traitants, liaisons sans-fil accessibles et nature de leur sécurité …), des protections périmétriques (pare-feu, antivirus …) et des dispositifs de sécurité (paramétrage, mots de passe, chiffrement …), etc.
- **Humaine** : toute information sur les dirigeants et les administrateurs des systèmes d'information (organigrammes, noms et identifiants) et sur leurs relations personnelles et professionnelles, mauvaises pratiques de sécurité des administrateurs et des usagers, etc.
- **Organisationnelle** : organisation, procédures, plans et consignes de sécurité et de cybersécurité (politique de sécurité, procédures opérationnelles de sécurité, plans de continuité et de reprise d'activité), gestion des identités, des comptes informatiques et des droits d'accès, etc.

Etape 2 : la préparation de l'armement, la *« Weaponization »*

Les attaquants vont se constituer un « arsenal cyber ». Ils vont se lancer à la recherche d'outils spécifiques *(exploits),* trouvables notamment sur le DarkNet. Ils vont également faire l'acquisition de malwares spécifiques ciblant les systèmes d'information cibles. **Les précédents ont pu démontrer la dangerosité de ce type de malware. Celle-ci réside dans leur modularité et dans leur adaptabilité à la structure ciblée**. Ces malwares peuvent se maintenir dans le réseau, interférer directement avec les systèmes critiques de l'organisation, exploiter les vulnérabilités de leurs protocoles de communication et effacer les traces de leurs actions sur les journaux d'événements (log). Chaque malware peut être utilisé avec un certain nombre de modules additionnels (*launcher, data Wipe, keylogger, etc.*) afin d'amplifier les effets de l'attaque et de perdurer sur le système cible.

Les exemples qui suivent, inspirés des cyberattaques récentes, permettent de comprendre les particularités des malwares utilisés.

Premier exemple, lors de la cyberattaque ukrainienne de 2015, c'est une version récente du malware **BlackEnergy** qui a été utilisée par les pirates. Une de ses particularités était d'introduire un *KillDisk* dans le système d'information du réseau électrique, rendant possible la destruction définitive de toutes les données présentes sur les disques durs des postes de travail et des serveurs, y compris celles nécessaires pour démarrer les systèmes d'exploitation. Ce *KillDisk* était la charge utile qui a permis de provoquer la chute du réseau électrique. BlackEnergy permettait aussi de créer une porte dérobée (*backdoor*) donnant aux assaillants le moyen de dialoguer avec les modules malveillants installés sur les ordinateurs infectés, et notamment avec la charge utile.

Le malware **Industroyer/CrashOverRide**[30]**,** utilisé lors de la cyberattaque du réseau électrique de Kiev en 2016, constitue un exemple parlant. Il a permis aux hackers de communiquer et de contrôler directement les équipements du centre de distribution (relais, coupe-circuit, interrupteurs, disjoncteurs). Un module supprimait ses traces, le rendant indétectable par les responsables de la sécurité du système.

Enfin, **Triton/Trisis,** récemment découvert par des chercheurs en cybersécurité, est un malware qui s'attaque spécifiquement au système Triconex produit par Schneider Electrics et largement vendu dans le monde pour assurer la sécurité des installations industrielles. Ses concepteurs auraient effectué de l'ingénierie inverse du code de Schneider pour cartographier le système et trouver la vulnérabilité qu'ils ont exploitée.

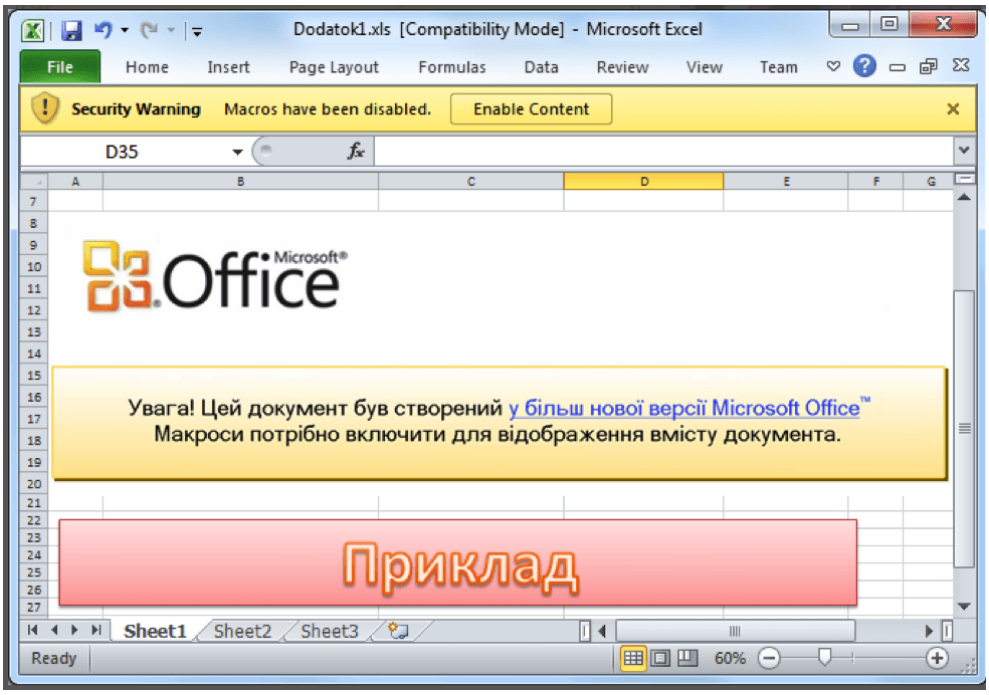
Etape 3 : l'introduction du malware dans le système

L'introduction d'un malware dans un système d'information peut se faire de plusieurs manières, en exploitant les failles humaines, organisationnelles et techniques de l'organisme. Les attaquants peuvent ainsi compromettre le système d'information :

- **A distance**, en exploitant ses vulnérabilités et en injectant du code malveillant *(exploitation de vulnérabilités logicielles, introduction dans le système de paiement en ligne des usagers qui permet ensuite un accès privilégié aux contrôles centralisés sur les serveurs, compromission du système d'information des sous-traitants et des partenaires pour accéder à celui de l'ICS) ;*
- **Par accès direct au système de l'organisme cible**, soit en accédant physiquement à une machine et en utilisant une clef USB infectée, soit via un réseau wifi non ou mal protégé ;
- **Ou par l'envoi de mails piégés aux employés de l'entreprise**, sous forme de campagnes de phishing ou, plus discret, par un mail spécifiquement conçu pour leurrer une personne précise en prenant l'apparence d'un mail légitime.

C'est ce dernier scénario qui a permis de compromettre en 2015 le système d'information du fournisseur d'électricité ukrainien Prykarpattya Oblenergo. Le malware BlackEnergy a été intégré dans des documents Microsoft Office envoyés par mail à des employés de l'entreprise, sous couvert d'un émetteur légitime (autorité étatique, organisation officielle, …). Une fenêtre pop-up invitait le destinataire à activer les macros sur le document (voir l'illustration ci-dessous). Le malware s'exécutait alors sur le réseau de l'entreprise. Cette attaque n'a nécessité aucune exploitation de vulnérabilité, puisqu'elle utilisait les fonctionnalités déjà disponibles du système.

[30] *Respectivement, les noms donnés au malware par ESET et Dragos.*



Source : www.numerama.com

Etape 4 : l'exécution

Une fois introduit dans le système de la cible, **le code du malware s'exécute** afin d'exploiter les vulnérabilités du système.

Etape 5 : l'installation :

Après son exécution, le malware va s'installer pour atteindre peu à peu le système de contrôle industriel ciblé et y déposer sa charge utile. Dans certains cas, il ne fera qu'ouvrir une faille dans le système pour pouvoir y revenir ultérieurement *(backdoor)*. En général, il s'installera de manière durable et déroulera son programme pour mettre en place un accès distant continu (*persistent access*), accéder à de nombreuses informations sensibles sur le fonctionnement général du système d'information, créer ou usurper un compte d'utilisateur et en augmenter les privilèges, acquérir ainsi des droits élargis d'accès et de modification du paramétrage de sécurité du système, pour modifier par exemple des certificats de sécurité, installer des outils supplémentaires, se déplacer latéralement dans le système, masquer ses traces, et in fine, atteindre le système industriel ciblé.

Comme dans le cas de BlackEnergy, le malware peut comporter un Shell, c'est-à-dire un interpréteur de commandes qui lui permettra d'exécuter des commandes et de mener les diverses actions de cette étape.

Etape 6 : Command and Control :

En parallèle à l'installation du malware, les attaquants vont mettre en place la capacité de commander le malware, de récupérer l'information qu'il extrait et d'accéder à distance à toutes les commandes du système d'information cible. De cette manière, ils pourront interagir directement avec celui-ci, évaluer précisément le

résultat des actions du malware, les réorienter si nécessaire, tester discrètement sa capacité à atteindre l'objectif de l'attaque, puis ordonner l'attaque finale.

Cette capacité de Command and Control peut être assurée directement depuis les locaux des attaquants, mais le plus souvent, pour interdire de remonter jusqu'à eux lors des investigations postérieures à l'attaque, ils feront transiter la liaison par un ou plusieurs ordinateurs qu'ils auront précédemment compromis dans différents pays choisis pour leur faible niveau en cybersécurité et en lutte contre la cybercriminalité.

Etape 7 : l'attaque

Une fois les étapes précédentes achevées, les attaquants vont pouvoir déclencher la phase finale, la coupure d'électricité, par un ordre donné à la charge utile de provoquer l'action prévue contre les installations de contrôle industriel.

En général, des actions seront menées en parallèle sur le système d'information pour masquer l'attaque et rendre la plus longue et complexe possible la restauration de l'alimentation électrique : prise de contrôle totale des postes de travail, interdiction d'accès des opérateurs de l'organisme cible à leur propre système, mise des systèmes informatiques hors d'état de fonctionner par effacement des programmes de démarrage du système d'exploitation, coupure des réseaux ou toute autre mesure permettant de provoquer une panne informatique généralisée.

> ***"Destructive malware attacks are simple and fast to execute. In many cases, once the user knows that something odd is occurring on the system, it is already too late to do anything about it. "***
> ***Industrial control system cyber emergency response team – USA***

Une cyberattaque de cette nature peut avoir des conséquences très graves. Bien au-delà de l'impact négatif d'une couverture médiatique mondiale sur la réputation du pays, une coupure électrique longue d'une grande ville ou d'une large région pourra entraîner une crise de grande ampleur : crise politique, par l'affaiblissement des sphères décisionnaires de l'Etat, incapables d'assurer la sécurité des opérateurs d'importance vitale et donc la continuité des services publics et des fonctions socio-économiques vitales ; crise humanitaire par arrêt des services d'urgence non dotés de plans et de moyens de continuité suffisants ; accidents en série du fait de l'interruption des systèmes de régulation et de sécurité des transports ; panique de la population ; pertes de vies humaines, etc.

Les répercussions financières sont directes, il s'agit des frais de remise en service du système électrique. Elles sont aussi indirectes, l'activité économique du pays étant suspendue le temps de la remise en continuité. La perte de gain est inévitable. Pour l'entreprise fournissant l'électricité, le risque image est très fort, elle est perçue comme ne pouvant assurer sa mission principale et responsable de ne pas avoir été résiliente. Le

risque juridique est à prendre en compte, la perte d'électricité causant des dégâts qui peuvent faire l'objet de demandes d'indemnisations.

En outre, l'impact de l'attaque peut être aggravé par d'autres actions conduites en parallèle par les attaquants ou leur commanditaire. La transmission de fausses informations peut alimenter la panique générale. Des attaques en déni de service sur les réseaux téléphoniques peuvent être menées pour empêcher les autorités et les opérateurs de connaître l'étendue des dégâts, et amplifier ainsi le chaos.

A moyen terme, les tensions préexistantes entre la population et l'Etat peuvent alors s'envenimer. C'est d'ailleurs le moment que peuvent choisir les hackers pour revendiquer leurs actions. Leur message peut retentir d'autant plus fortement dans ce contexte. Les conséquences géopolitiques sont très importantes. Il existe une forme de pression de la population et des médias tenant à l'attribution de l'attaque à un pays en particulier. Il est possible que la crise communicationnelle et les accusations à tort aient pour conséquence la détérioration des relations avec d'autres Etats.

L'action des acteurs régaliens et des entreprises pour faire face aux cybermenaces

Comme dans tous les domaines de la sécurité et de la résilience de la nation, des mesures doivent être prises tant par l'Etat que par les opérateurs concernés pour limiter au maximum les risques de coupures électriques par des cyberattaques, réduire leur impact et faciliter une reprise rapide de l'activité. La France est, de ce point de vue, relativement bien protégée par l'action de l'Etat, auquel s'ajoute le cadre législatif mis en place par l'Union européenne, plus particulièrement important dans le domaine de l'énergie électrique du fait de l'interconnexion des réseaux des différents Etats membres.

De nombreuses mesures concrètes ont été prises par l'Etat et par l'Union européenne pour améliorer la cybersécurité et la résilience de leurs installations propres et au-delà, de celles des rouages socio-économiques nationaux (structures responsables de la cybersécurité et de la cyberdéfense, formation, recherche, labellisation de sécurité des produits et services, plans et moyens de continuité de l'Etat, etc.). Ne sont cependant détaillées ci-dessous que les principales mesures de nature juridique mises en place par la France et l'UE.

Le cadre légal français

En France, les principaux fournisseurs d'électricité sont désignés Opérateur d'importance vitale (OIV), dans la mesure où une interruption de leur activité aurait des conséquences graves sur la capacité de survie de la Nation[31]. Sur les 249 opérateurs d'importance vitale répartis en 12 secteurs d'activité[32], 21 appartiennent au secteur de l'énergie.

---

[31] *La notion d'opérateur d'importance vitale est définie par l'article L1332-1 du code de la défense : « Les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation, sont tenus de coopérer à leurs frais dans les conditions définies au présent chapitre, à la protection desdits établissements, installations et ouvrages contre toute menace, notamment à caractère terroriste».*

[32] *Code de la défense : articles L1332-1 à L1332-7 et R1332-1 à R1332-42.*

Parmi les nombreuses mesures destinées à renforcer leur protection et leur résilience[33], ces opérateurs ont l'obligation de se conformer aux dispositions mises en place par la loi de programmation militaire de 2013. Ils doivent identifier, **déclarer et renforcer leurs systèmes d'information d'importance vitale (SIIV), déclarer les incidents, mettre en œuvre les règles de sécurité spécifiques prévues par arrêté[34], et avoir recours à des produits et des prestataires qualifiés par l'ANSSI.**

Le cadre légal de l'Union Européenne

La directive du Conseil sur les infrastructures critiques européennes du 8 décembre 2008[35] instaure un mécanisme visant à identifier les infrastructures critiques européennes, notamment dans les secteurs de l'énergie et constitue un cadre pour améliorer la sécurité des grandes infrastructures à vocation transnationale et la résilience à l'échelle de l'Union européenne. En effet, l'impact d'une cyberattaque nationale peut s'étendre à plusieurs pays de l'UE. Par ailleurs, un programme européen est dédié à la protection des infrastructures critiques européennes et nationales[36].

En complément, l'Union européenne a émis diverses recommandations visant à renforcer la protection des infrastructures d'information critiques[37].

Elle s'est dotée en 2013 d'une stratégie de cybersécurité[38], suivie en 2016 d'une directive, dite NIS (Network and Information Security)[39], instaurant des "mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union". Cette directive prévoit qu'avant le 9 mai 2018, les Etats membres fixent des exigences en matière de sécurité et de notification pour les opérateurs de services essentiels (OSE), parmi lesquels notamment les opérateurs d'énergie. Très inspirée du dispositif en vigueur en France pour les OIV, elle n'entraînera pas de changement notable pour les OIV français, mais va largement étendre le périmètre des opérateurs de production et de distribution électrique concernés par les futures mesures de cybersécurité.

L'action des opérateurs

Avec les mesures qui leur seront prochainement imposées en application de la directive NIS, les opérateurs de production et de distribution électrique non OIV disposeront d'un cadre d'action précis, probablement d'un niveau proche de celui déjà demandé aux OIV.

---

[33] *Telles que prévues par l'instruction générale interministérielle relative à la sécurité des activités d'importance vitale, l'IGI n°6600 du 7 janvier 2014.*

[34] *Arrêté du 11 août 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « Approvisionnement en énergie électrique ».*

[35] *http://eur-lex.europa.eu/legal-content/FR/ALL/?uri=celex:32008L0114*

[36] *http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=LEGISSUM%3Al33260*

[37] *Communication de la Commission relative à la protection des infrastructures d'information critiques - « Protéger l'Europe des cyberattaques et des perturbations de grande envergure : améliorer l'état de préparation, la sécurité et la résilience », http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2009:0149:FIN*

[38] *http://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:52013JC0001*

[39] *http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016L1148*

Le développement rapide de systèmes d'information très novateurs dans les réseaux de régulation et de distribution électrique, avec notamment le déploiement en cours des compteurs Linky, nécessite par ailleurs un engagement déterminé de tous les opérateurs concernés. Au-delà des exigences à venir, ils devront a minima sensibiliser et former leur personnel, faire respecter les règles d'hygiène informatique définies par l'ANSSI, cloisonner au mieux les diverses parties de leurs systèmes d'information, définir des dispositions techniques et organisationnelles de détection, et établir de réels plans de continuité et de reprise d'activité.

L'objectif est de compliquer l'exécution des différentes étapes de la KillChain, de détecter autant que possible les actions conduites à chaque étape par un attaquant, et, en cas d'attaque réussie, d'en limiter au mieux l'impact et de restaurer au plus vite la distribution électrique.

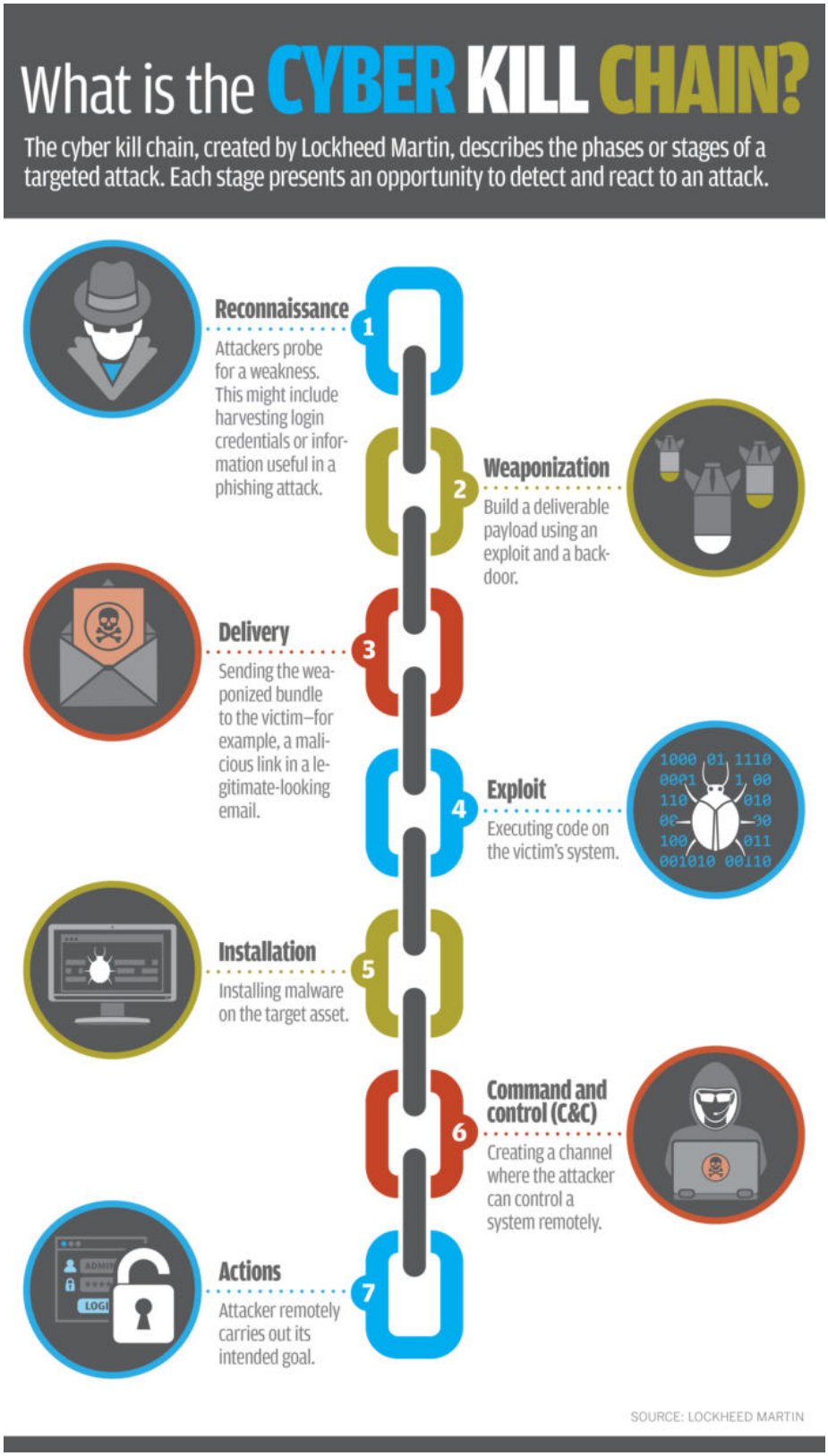
Conclusion

Les attaques visant à priver d'électricité une région ou un pays sont des opérations qui demandent un investissement important en expertise, temps et argent. Elles ne proviendront a priori que de structures étatiques ou de grands groupes cybercriminels, les seuls à pouvoir consacrer les ressources nécessaires pour atteindre leur objectifs politiques ou idéologiques.

Se protéger de telles attaques est plus complexe encore et nécessite des investissements financiers, techniques et humains élevés. En Europe, les actions découlant des démarches européennes et nationales de sécurisation des opérateurs d'importance vitale, et bientôt des opérateurs de services essentiels, sont de nature à limiter les risques, bien que le risque zéro n'existe pas, tout particulièrement en matière cyber. Les opérateurs doivent prendre leur part, a minima en faisant au mieux ce qui est imposé par les cadres législatifs.

On peut toutefois s'étonner du faible nombre de réelles coupures d'électricité qui ont eu lieu jusqu'aujourd'hui. En effet, les chercheurs de Symantec ont confirmé que les fournisseurs d'électricité de plusieurs pays, dont la France, ont déjà été impactés par les premières étapes de la KillChain dès 2013. Les attaques menées avaient-elles alors des objectifs moins ambitieux que de priver d'électricité une population ? Ou alors, les attaquants ont-ils échoué à atteindre leur but ? Gageons, avec modestie, que le nombre finalement restreint d'attaques ainsi que l'absence d'incidences plus dramatiques sont la conséquence des mesures de cybersécurité mises en place notamment par les pouvoirs publics. Cela doit encourager tous les opérateurs concernés à poursuivre les efforts.

Annexe : La cyber Kill Chain (Source : Lockheed Martin)



La **Direction Générale des Relations Internationales et de la Stratégie (DGRIS)** propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation. Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique**, sous le numéro de marché 1502492543. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère des Armées
Direction Générale des Relations Internationales et de la Stratégie
60 Boulevard du Général Martial Valin – CS21623 – 75 509 Paris Cedex 15

CEIS
Tour Montparnasse – 33, avenue du Maine – BP 36 – 75 755 - Paris Cedex 15
Téléphone : 01 45 55 00 20
E-mail : omc@ceis.eu