

# Le leurrage numérique: taxonomie et cadre juridique – une étude de cas suisse

Bastien Wanner<sup>1</sup> et Solange Ghernaoui<sup>2</sup>

<sup>1</sup> Département des systèmes d'information, HEC Lausanne, Université de Lausanne, 1015 Lausanne, Suisse

<sup>2</sup> Swiss Cybersecurity Advisory & Research Group, Université de Lausanne, 1015 Lausanne, Suisse

`bastien.wanner@unil.ch`

## Abstract.

Le leurrage numérique est un ensemble de techniques ayant pour but soit d'attirer l'attaquant afin de collecter des informations sur ses tactiques, techniques et procédures (par exemple avec un *honeypot* qui simule), soit de gêner l'attaquant dans la réussite de son attaque en le trompant et le désorientant (par exemple avec un *decoy* qui dissimule). Ce type de mesures, qui est déployé au sein des systèmes et réseaux informatiques à protéger, est en interaction avec l'attaquant et tente de modifier son comportement. Dans la littérature, les mesures actives de cyberdéfense font référence à des actions – quasi-offensives – effectuées en dehors du périmètre de sa propre infrastructure informatique et surtout cherchant à obtenir un effet, si possible perturbateur, au plus proche de la source d'une attaque afin de la faire cesser. Cet article a pour but de définir la taxonomie du leurrage numérique et de débattre s'il peut être qualifié de mesures actives de cyberdéfense soulignant les opportunités et risques engendrés. Une analyse du droit international et national suisse applicable au leurrage numérique complète la discussion. Cet article conclut sur quelques recommandations et sur des pistes de perspectives futures. Un éclairage particulier est apporté sur les obligations juridiques relatives à l'encadrement de ces mesures de leurrage numérique.

**Keywords:** cyber defence, active defensive measures, deceptive security, honeypots, international law

## 1 Introduction

De nombreuses techniques ont été développées pour augmenter la vitesse et la précision des activités de détection d'intrusion dans le but de renforcer les barrières de sécurité et les lignes de défense d'un système d'information et de ce fait rendre le travail du défenseur plus efficace. Mais peu de recherches ont été effectuées sur les mécanismes qui rendent plus difficile la vie de l'attaquant et perturbent sa capacité à atteindre ses objectifs. Les techniques de cyberprotection basiques ne font que bloquer les accès de l'attaquant de manière à ce qu'il perde son temps et son énergie (Ferguson-Walter et al., 2017). Les techniques de leurre dans le domaine cyber ont donc émergées pour compléter la panoplie de cybersécurité en influençant et déstabilisant l'attaquant. Dans le domaine cyber, l'attaquant ne connaît seulement que ce qu'il peut lui-même percevoir à travers le réseau ciblé (Ferguson-Walter et LaFon, 2015). Par conséquent, le propriétaire du réseau a la possibilité de révéler à l'attaquant les informations qu'il désire – y compris des informations destinées à tromper (déception) l'attaquant. Dans la mesure où les réseaux informatiques et les systèmes d'information sont complexes, ils constituent un contexte idéal pour réaliser des actions de déception afin de pouvoir tenter de contrôler les connaissances de l'attaquant (Ferguson-Walter et al., 2017). Cela permet ainsi au défenseur de choisir quelles ressources il souhaite montrer à l'attaquant, selon une stratégie de sécurité et de défense préalablement déterminée afin de garder à distance et de mieux contrôler ses adversaires potentiels.

Deux approches existent pour faire face à des accès non autorisés et des intrusions dans un système d'informations. L'une s'appuie sur la détection et la réponse aux incidents et l'autre est basée sur la déception par des actions défensives sur les réseaux informatiques (*deceptive computer network defense*) (Heckmann et al., 2013). Dans la première approche, l'action de cybersécurité consiste essentiellement à protéger les ressources par la détection des incidents de sécurité, la gestion des droits d'accès, la gestion des vulnérabilités, la journalisation des événements (*logs*), ainsi que la gestion des sauvegardes (Gheraoui, 2013). La seconde approche basée sur la déception diffère dans la mesure où il s'agit d'attirer l'attaquant dans les filets de la défense en exposant délibérément des systèmes afin qu'ils soient prioritairement sondés, attaqués et compromis par l'adversaire.

Le but de cet article est de clarifier le concept de leurrage numérique qui n'est pas défini dans la littérature. Est-ce que le leurrage numérique peut être considéré comme des mesures actives de cyberdéfense et donc est soumis aux réglementations l'encadrant ? Sinon, quels autres cadres légaux s'appliquent aux mesures de leurrage numérique ? Premièrement une revue de la littérature est effectuée afin de définir la taxonomie de la déception et du leurrage numérique. Des définitions et caractéristiques des mesures passives et actives de cyberdéfense sont proposées. Deuxièmement, le cadre juridique du leurrage numérique est analysé, en particulier les domaines du droit international public et du droit national public suisse relatif à la cybersécurité. Troisièmement, une taxonomie du leurrage numérique est proposée et les obligations légales du leurrage sont analysés détaillant ce qui est autorisé et ce qui est interdit en droit international et

en droit national suisse. Enfin, quelques recommandations sont émises et des pistes de perspectives futures sont élaborées.

Cet article ne traite pas de la problématique de la provocation à l'infraction qui est parfois reproché au leurrage numérique. Il ne traite pas non-plus en détails des problématiques de respect de la vie privée et de protection des données qui sont des problématiques de droit privé. Enfin, sachant que cet article analyse principalement la problématique sous l'angle du droit public, les éléments analysés seront issus du secteur gouvernemental et non pas du secteur privé.

## 2 Analyse de la littérature

Le leurre numérique n'est pas défini dans la littérature. Selon le Larousse, un leurre est "ce sur quoi on aurait tort de se fonder, ce qui trompe". Un leurre, peut être considéré comme une simulation dont la finalité est de tromper pour se protéger ou pour constituer un appât. Très utilisé dans la nature par différentes espèces animales qui changent de couleur ou de forme pour imiter leur environnement (Smith, 2005), l'homme s'en est inspiré pour l'étude ou le dressage des animaux, pour la chasse et la pêche ou encore dans le domaine militaire.

### 2.1 Définition du concept de déception

Le leurrage numérique est une traduction française du concept de *deceptive security*. Ce type de mesure de sécurité fait référence à la tromperie, la supercherie, la duperie ou encore à l'imposture dans le but d'augmenter l'efficacité de la sécurité. C'est un concept que le domaine militaire utilise également depuis des siècles dans ce qui est nommé la déception. Sun Tzu en fait déjà de nombreuses références dans son célèbre ouvrage de stratégie *L'Art de la guerre*. Ferguson-Walter et al. (2017) proposent une définition: "la déception est la fourniture d'informations erronées suffisamment réalistes pour embrouiller la conscience de la situation d'un adversaire, pour influencer et détourner les perceptions et les processus de décision de l'adversaire". L'OTAN (2019) propose une autre définition de la déception: "Mesures visant à induire l'adversaire en erreur, grâce à des truquages, des déformations de la réalité, ou des falsifications, en vue de l'inciter à réagir d'une manière préjudiciable à ses propres intérêts". Des techniques de déception ont été utilisées dans de nombreux conflits et leurs applications ont été étudiées et également théorisées depuis plusieurs décennies. Whaley (1969) a défini les types de tromperie utilisés dans les opérations militaires cinétiques à travers les âges, y compris la dissimulation du réel par le masquage et le reconditionnement, ainsi que l'éblouissement et la révélation du faux par l'imitation, l'invention et le leurre. De Faveri et al. (2018) présentent les principaux concepts basés sur la déception. Selon Bell et Whaley (1991), il s'agit d'un processus par lequel des actions délibérées sont utilisées pour induire des conclusions erronées. Il y a deux grandes catégories d'actions de la déception: la simulation qui est le fait de monter le faux et la dissimulation qui est le fait de cacher le vrai (Bell et Whaley, 1991). Ces actions induisent des biais dans la perception de l'autre, ce qui influence l'état d'esprit, la prise de décision, la confiance, les croyances

et le comportement (Hilbert, 2012). La cible finale est de porter atteinte à l'esprit de l'adversaire (Ormrod, 2014).

## 2.2 Définition du concept de leurrage numérique

En cybersécurité, la même taxonomie a été reprise et le leurrage numérique (ou cyber-déception) repose sur deux principaux types d'artefacts : le *honeypot* et le *decoy*.

Le *honeypot* (pot de miel) est considéré comme une technique primaire, dont la tâche principale consiste, comme son nom l'indique, à attirer l'attaquant afin de connaître ses tactiques (Spitzner, 2003). Ces *honeypots* sont fait pour être attaqués afin de collecter des informations sur les tactiques, techniques et procédures (TTP) de l'attaquant (Provos, 2004) et de détourner celui-ci de la cible réelle en la masquant. Ces *honeypots* peuvent être classés, selon leur niveau d'interaction avec l'adversaire, dans deux catégories : basse interaction et haute interaction. Les *honeypots* de basse interaction émulent certaines caractéristiques restreintes d'un système d'exploitation ou de services réseaux (Sokol et al., 2017). Alors que les *honeypots* haute interaction sont des systèmes d'exploitation complets, incluant tous les services : rien n'est restreint ni émulé (Sokol et al., 2017). Spitzner (2003) propose également une classification par intention : des *honeypots* de recherche et de production. Des *honeypots* de recherche servent uniquement à obtenir des informations sur l'attaquant mais n'ont pas de plus-value directe pour la cybersécurité d'une organisation. Ceux de production sont utilisés dans l'environnement informatique d'une organisation et servent à atténuer les risques. Des *honeypots* regroupés en réseaux sont appelés *honeynet* et sont généralement composés de plusieurs ordinateurs qui interagissent plus ou moins avec l'attaquant selon ce qui est souhaité (Spitzner, 2003). Un *honeynet* est composé de quatre éléments principaux relatifs aux données : le contrôle, la capture, la collecte et l'analyse (Sokol et al., 2017). Selon Heckmann et al. (2013), il y a également des *fake honeypots* qui sont des vraies machines avec des artefacts de faux systèmes, afin de tromper l'attaquant en lui faisant croire que le système attaqué n'a pas de valeur (Rowe et al., 2006). Ou encore, par récursivité, il y a des *fake fake honeypots* (Heckmann et al., 2013) qui contiennent le même type d'artefacts mais qui sont de vrais *honeypots* (Rowe et al., 2007). Enfin, une autre approche consiste à utiliser de vrais systèmes informatiques qui sont alimentés par de fausses informations appelées *honeytokens* (Spitzner, 2003). Ces *honeytokens* servent à détecter des intrusions par des utilisateurs non autorisés (Qassrawi et Hongli, 2010) et ainsi à éviter des écoutes clandestines (Chakravarty et al., 2011). En résumé, le *honeypot* a pour but d'attirer l'attaquant ailleurs sur un système volontairement peu protégé afin de l'éloigner d'une cible de valeur et de récolter des informations sur la menace que représente cet attaquant (Provos, 2004 ; Vrabie et al., 2005).

Le *decoy* (leurre, appât) diffère du *honeypot* (Bringer et al., 2012). Le *decoy* est directement intégré dans le vrai réseau opérationnel et a également comme but de collecter des informations sur l'attaquant. Mais le principal objectif du *decoy* est de mettre l'attaquant dans la confusion et de masquer la vraie typologie du réseau (Ferguson-Walter et al., 2017), ce qui a pour finalité de le ralentir ou de l'empêcher de déployer son attaque. Ainsi la différence fondamentale est que le *honeypot* attire l'attaquant en ayant l'air plus séduisant que les véritables systèmes qui ont de la valeur, alors que le

*decoy* rend les véritables valeurs (*assets*) plus difficiles à identifier en occupant un maximum d'espace possible et en déclenchant une alerte dès qu'un attaquant interagit avec (Ferguson-Walter et al., 2017). L'objectif final étant de procurer un avantage asymétrique au défenseur. Cela permet de réduire le risque que les véritables valeurs soient attaquées en distrayant l'attaquant, en le forçant à entreprendre des actions supplémentaires, en le ralentissant ou en augmentant la probabilité qu'il soit détecté plus rapidement (dans la *cyber kill chain*) et perturbant ainsi sa progression (Ferguson-Walter et al., 2017).

En résumé, le leurrage numérique a deux finalités : collecter des informations sur l'attaquant et le gêner dans ses attaques en le désorientant (Ferguson-Walter et al., 2017). Cela permet de renverser l'asymétrie préexistante entre l'attaquant et le défenseur. Ces techniques ont comme fondement l'interaction avec l'esprit humain de l'attaquant et elles tirent profit des biais des comportements humains. Des études ont également démontré que le simple fait que l'attaquant suspecte la présence de techniques de déception, agit déjà sur son comportement. Le leurrage numérique aurait par nature, une sorte d'effet dissuasif.

### 2.3 Définitions des mesures passives et actives de cyberdéfense

Dans la littérature, les techniques de leurrage numérique sont souvent qualifiées de proactive. En cyberdéfense, une distinction est faite entre les mesures passives et actives de défense dans le cyberspace. Le manuel de Tallin (Schmitt, 2017) du *NATO's Cooperative Cyber Defence Centre of Excellence* (CCD COE) fait clairement cette distinction. La cyberdéfense passive est la "prise de mesures pour détecter et atténuer les cyberintrusions et les effets des cyberopérations qui n'impliquent pas le lancement d'une opération préventive, *pre-emptive* ou contre la source de l'attaque". Tous les outils de cybersécurité sont inclus dans cette définition, tels que les pare-feux, les correctifs, les antivirus ou encore les outils d'analyse numérique. A l'opposé, la cyberdéfense active est quant à elle la "prise de mesures de défense en dehors de l'infrastructure cyber défendue". Plus communément appelé *hackback*, les mesures actives de cyberdéfense ont pour objectif principal de prendre des mesures contre la source identifiée d'une cyberopération malveillante. Ce *hackback* est une action de piratage conçu pour atténuer les effets ou arrêter l'activité malveillante, ou pour obtenir des preuves techniques qui peuvent être utilisées à des fins d'attribution (Schmitt, 2017). Divers universitaires ont également proposé des définitions des mesures actives : "la cyberdéfense active est une action défensive directe prise pour détruire, annuler ou réduire l'efficacité des cybermenaces contre les forces et les moyens amis" (Denning and Strawser, 2014), "une série d'actions offensives dommageables ou destructrices, telles que le contre-piratage, qui engagent un adversaire pendant ou rapidement après une cyberattaque initiale" (Iasiello, 2014). Enfin, Rosenzweig (2014) décrit ces mesures comme la "capacité à détecter, analyser et atténuer les cybermenaces", soit le principe que "les victimes peuvent pirater les pirates qui les attaquent". Dans un autre article de Rosenzweig (2017), les mesures actives de cyberdéfense se divisent en trois catégories distinctes : la gêne, l'attribution ou l'attaque. La gêne est la moins agressive des formes de cyberdéfense active. Elle va au-delà des mesures passives de cyberdéfense mais reste toutefois localisé sur

le réseau du défenseur. Le leurrage numérique tomberait sous cette définition selon Rosenzweig.

## 2.4 Caractéristiques des mesures actives de cyberdéfense

Quelques universitaires (Kello, Dewar, Denning) ont proposé des caractérisations des mesures actives de cyberdéfense. Kello (2016) identifie trois aspects principaux : but défensif, emplacement hors périmètre et flexibilité tactique. Le but défensif consiste à empêcher de manière proactive l'attaquant mais sans le pénaliser pour autant. L'emplacement hors-périmètre est la capacité à agir en dehors de ses propres systèmes et réseaux : dans des domaines adverses ou neutres. Enfin la flexibilité tactique est l'éventail d'effets possibles sur les systèmes et réseaux adverses, allant de la collecte de renseignements à la perturbation (jusqu'à la destruction). L'élément central qui rend ce concept actif est le fait que l'action défensive se déroule en dehors du périmètre des systèmes et réseaux du défenseur. En outre, la réponse doit être réactive, directe et en temps-réel (Wanner et Ghernaouti, 2019). En d'autres termes, toute action visant les infrastructures TIC de l'adversaire ou d'une tierce partie, dans le but d'altérer, de réduire, d'annuler ou de détruire les capacités de l'attaquant d'effectuer la cyberattaque en cours, constitue une cyberdéfense active.

## 3 Le cadre juridique du leurrage numérique

Le cadre juridique du leurrage numérique fait depuis plusieurs années l'objet d'un débat académique (Spitzner, 2003; Barei, 2004). Il y a bien entendu le domaine du droit international public, mais aussi du droit national et en particulier du droit au respect de la vie privée et à la protection des données. Le droit au respect de la vie privée existe depuis des décennies dans de nombreux pays et sa conception plus ou moins exigeante diffère d'une région à l'autre en raison de l'histoire, des valeurs et de la culture des populations. Depuis quelques années, il y a eu plusieurs révisions de lois en matière de protection des données et cela pourrait être corrélé avec les récents scandales de collectes massives de données. La problématique de la protection des données dans le cadre du leurrage numérique a été largement étudié dans la littérature tant anglo-saxonne qu'européenne. Les débats se sont principalement concentrés autour de trois concepts fondamentaux : la vie privée, la responsabilité et l'incitation à commettre un délit (Spitzner, 2003). Le leurrage numérique est effectivement un outil qui collecte une grande quantité de données y compris des données personnelles. Dans l'article de Sokol et al. (2017), une analyse approfondie de ces concepts en lien avec les *honeypots* est effectuée. En résumé, ils affirment qu'il faut faire la distinction entre le contenu des données (contenu des communications) et les informations de transactions (nécessaire à établir la communication). Les gestionnaires de *honeypots* sont considérés comme des "responsables du traitement" des données personnelles et devraient donc se conformer à la législation en vigueur (e.g. RGPD). En outre, le concept d'intérêt légitime est capital pour la collection de données personnelles par un *honeypot* et une attention particulière devrait être apportée sur la durée de conservation des données. Enfin, dans le

partage ou la publication d'information, Sokol et al. recommandent l'anonymisation autant que possible. L'analyse dans ce chapitre ne va pas traiter plus en détails l'aspect du respect de la vie privée et de la protection des données en matière de droit privé, mais va se concentrer sur les aspects de droit public.

### 3.1 Droit international public

Dans le domaine du droit international public, un document qui fait référence est le manuel de Tallinn (Schmitt, 2017). Dans le chapitre 5 "cyberopérations qui ne sont pas *per se* régulées par le droit international", la règle 32 régit le cyberespionnage en temps de paix. Bien que le cyberespionnage par les États ne violent pas le droit international, la méthode choisie pour ce faire pourrait le violer. Le chiffre 15 est dédié au *honeypot*. Il est stipulé que des *honeypots* sont créés par les États en partant du principe que d'autres États mèneront des activités de cyberespionnage à leur rencontre. Ces *honeypots* peuvent être utilisés de diverses manières. Premièrement, un État en utilise à des fins de contre-espionnage pour surveiller la façon dont un autre État mène ses cyberopérations, fournissant ainsi des informations précieuses sur les comportements et les capacités cyber de cet État. Deuxièmement, un État peut stocker dans le *honeypot* des fichiers qui, une fois exfiltrés, lui fourniront des informations sur leur destination afin de pouvoir déterminer quels États s'adonnent à des activités de cyber-espionnage à son rencontre. Les fichiers exfiltrés peuvent également inclure la possibilité de surveiller les activités dans leur nouvel environnement. Selon le groupe d'experts internationaux ces opérations ne constituent pas des violations du droit international. Dans le premier cas, c'est simplement un exercice de droits souverains par l'État qui a créé le *honeypot* sur son propre territoire. Le second ne constitue pas non-plus une violation d'une norme de droit international coutumier (e.g. violation de la souveraineté) due à l'État exfiltrant car elle constitue un simple cyber-espionnage. Il n'y aurait pas de violation si l'État lui-même avait transmis les fichiers dans les systèmes informatiques de l'État exfiltrant. Le chiffre 16 détaille une situation plus complexe impliquant un *weaponised honeypot* contenant des fichiers pouvant servir d'arme qui, une fois exfiltrés, provoqueront des perturbations ou des dommages importants dans le système cible. Bien que la question juridique soit une question d'attribution, le groupe d'expert est divisé sur cette question. La minorité est d'avis que l'opération est attribuable à l'État qui a créé le *honeypot* conformément au droit de la responsabilité étatique parce que cet État l'a initié et l'opération se terminera comme il l'a prévu. Ainsi, une telle opération viole au moins la souveraineté de l'État cible car la nature destructrice de l'opération la qualifie comme telle. En d'autres termes, l'État qui a placé les fichiers armés dans le *honeypot* a commis un fait internationalement illicite. La majorité des experts a estimé que les organes de l'État qui a infiltré le *honeypot* ont effectivement rapatrié des fichiers infectés dans leurs propres réseaux ; par conséquent, l'État qui a posé le *honeypot* n'a pas effectué l'action de transmettre des maliciels destructeurs dans l'infrastructure de l'État cible causant ainsi un dommage. Cette cyberopération ne lui est donc pas attribuable (Schmitt, 2017).

Dans le même manuel, la règle 123 concerne les ruses et stipules que les cyberopérations qui sont considérées comme des ruses de guerre sont autorisées. Cette règle est tirée de l'article 37 du Protocole additionnel I des Conventions de Genève qui stipule

que la perfidie est interdite, mais que les ruses de guerre ne sont pas interdites. Ces dernières sont des actes destinés à tromper l'adversaire ou à inciter les forces adverses à agir de manière imprudente, mais qui ne violent pas le droit des conflits armés. Elles ne sont pas perfides car ils n'invitent pas à la confiance de l'adversaire en ce qui concerne un quelconque statut protégé. Le manuel de Tallin (Schmitt, 2017) donne quelques exemples de ruses de guerre informatique autorisé : la création d'un système informatique "factice" simulant des forces inexistantes, transmission de fausses informations faisant croire à tort que des opérations sont sur le point de se produire ou sont en cours, utilisation de faux réseaux informatiques (par exemple, *honeynets*), fausses déclarations d'ordre émises par le commandant adverse, activités de guerre psychologique, transmission de fausses informations de renseignement destinées à être interceptées. Un élément commun de ruse de guerre est la présentation à l'adversaire de "fausse apparence que ce qui se passe réellement, permettant d'obtenir légalement un avantage militaire". Un exemple proposé par Schmitt (2017) serait l'utilisation d'un *decoy* pour tromper l'adversaire. En réponse à un malicieux, le *decoy* dévie les cyberopérateurs de l'adversaire en redirigeant leur attention vers un *honeypot* qui contient de fausses données qui semblent avoir une plus grande valeur militaire que celles qui étaient ciblées. Cette action est une ruse légale. Il est permis de camoufler des personnes et des objets, y compris dans un environnement civil, à condition que cela ne constitue pas un acte de perfidie. Le groupe international d'experts était toutefois divisé quant à la question de savoir s'il serait licite de camoufler un système ou réseau informatique dans un système civil d'une manière qui ne constitue pas un acte de perfidie. Par exemple, un système informatique militaire pourrait être hébergé dans un *cloud* public afin de paraître de nature commerciale pour le rendre plus difficile à détecter. La majorité des experts a estimé que cela serait illégal si l'opération portait atteinte au principe de distinction (règle 93) en faisant courir un risque accru aux civils et aux biens de caractère civil. La minorité a suggéré que seule la règle de la perfidie s'applique à de tels cas (Schmitt, 2017).

### 3.2 Cadre juridique suisse

Le cadre juridique suisse régle les activités du cyberspace depuis une dizaine d'années. Il y a le code pénal suisse (CP) qui sanctionne les infractions contre le patrimoine (art. 143 CP) et en particulier la soustraction de données et l'accès indu à un système informatique. Mais il y a aussi les nouvelles lois sur le service de renseignement (LRens) entrée en vigueur en 2017 et sur l'armée et l'administration militaire (LAAM) entrée en vigueur en 2018. Ces deux lois régulent, entre autres, les mesures actives de cyberdéfense. L'article 26 al. 1 let. d (LRens) stipule que l'infiltration dans des systèmes et des réseaux informatiques dans les buts de (1) rechercher des informations qu'ils contiennent ou qui ont été transmises à partir de ces systèmes ou (2) perturber, empêcher ou ralentir l'accès à des informations est soumis à autorisation. Il est également précisé que ces mesures sont exécutées secrètement et à l'insu des personnes concernées. L'article 37 (LRens) est la base légale autorisant l'infiltration dans des systèmes et réseaux informatiques. Mais pour ce faire, il y a trois conditions à remplir : (1) les systèmes et réseaux informatiques doivent se situer à l'étranger ; (2) ils doivent être



utilisés pour attaquer des cibles en Suisse ; (3) ces cibles doivent être des infrastructures critiques (selon la liste officielle de l'office fédéral de la protection de la population). Si ces trois conditions sont remplies, alors le service de renseignement de la confédération (SRC) peut infiltrer ces systèmes et réseaux informatiques afin de perturber, empêcher ou ralentir l'accès à des informations. C'est le Conseil fédéral (au minimum une majorité de 4 ministres sur 7) qui décide de la mise en œuvre de cette mesure. L'alinéa 2 de l'article 37 (LRens) légifère les infiltrations dans des systèmes et réseau informatiques étrangers dans le but de rechercher des informations. Ces mesures sont décidées par la cheffe du département de la défense, après consultation du chef des affaires étrangères ainsi que de la cheffe de la justice et la police. D'un point de vue militaire et en temps de paix, c'est l'article 100 (LAAM) qui régit les mesures actives de cyberdéfense. Le chiffre c. de l'alinéa 1 autorise les forces armées à s'introduire dans les systèmes et réseaux informatiques – servant à mener des cyberattaques contre l'armée – afin de perturber, empêcher ou ralentir l'accès à des informations. C'est également le Conseil fédéral qui décide de la mise en œuvre de ces mesures sauf en cas de service actif. Tant le SRC que l'armée sont autorisées à traiter des données personnelles, des données sensibles et des profils de la personnalité, y.c. à l'insu des personnes concernées, à condition et aussi longtemps que leurs tâches l'exigent.

Dans le cadre de la première stratégie nationale de gestion des cyberrisques (SNPC) de 2012 (UPIC, 2012), un projet de loi fédérale sur la sécurité de l'information (LSI) a été initié en 2014. Ce projet de loi définit les exigences minimales auxquelles toutes les autorités de la Confédération doivent répondre pour protéger leurs informations et infrastructures informatiques. Depuis 2017 cette loi (DDPS, 2017) est débattue au parlement fédéral et ballotté entre la chambre basse et la chambre haute du parlement. Dans un rapport explicatif sur ce projet de loi (Admin, 2014), il est explicitement mentionné que : "Les services chargés de tâches liées à l'article 75 al. 2 sont aussi autorisés à simuler des systèmes vulnérables (*honeypots*) sur des réseaux afin d'améliorer leurs connaissances". L'article 75 concerne le soutien de la Confédération aux exploitants d'infrastructures critiques. Ce soutien peut prendre les formes suivantes : (1) identification et évaluation des menaces, dangers, vulnérabilités et failles de sécurité ; (2) identification des incidents ; (3) maintien et rétablissement de la sécurité de l'information après un incident ; (4) suivi des incidents. Pour ce faire, la Confédération gère un service national d'alerte (MELANI – Centrale d'enregistrement et d'analyse pour la sûreté de l'information) et un service d'assistance (GovCERT). Avec l'adoption de l'ordonnance sur la protection contre les cyberrisques dans l'administration fédérale (OPCy, 2020) au 1er juillet 2020, ces deux entités ont été regroupées sous un même toit lors de la création du Centre national pour la cybersécurité (NCSC). Les lois et ordonnances relatives à la cybersécurité indiquent que le traitement des données personnelles est autorisé pour les services étatiques dont les tâches le requièrent. Ces données peuvent être traitées à l'insu de la personne concernée et, si elles sont utiles à la sécurité de l'information, elles peuvent être communiquées aux exploitants d'infrastructures critiques et aux fournisseurs de services informatiques. Ces derniers peuvent également fournir des données personnelles à la Confédération. Enfin, les données peuvent être échangées avec des services étrangers ou internationaux chargés de la protection

d'infrastructures critiques pour autant que cela soit nécessaires pour accomplir des tâches de cybersécurité. La durée de conservation des données est de cinq ans au plus.

## 4 Analyse

### 4.1 Le leurrage numérique : des mesures passives proactives de cyberdéfense

Dans la littérature, il y a un consensus sur le fait que les techniques de leurrage numérique font partie des techniques évoluées de cybersécurité. En effet, les principes basiques de la cyberprotection consistent à renforcer la robustesse des systèmes et réseaux avec tous les moyens passifs de cybersécurité décrit précédemment. Dans ce contexte, est-ce que le leurrage numérique peut être considéré comme des mesures actives de cyberdéfense ? Nous postulons que non. Certes le leurrage numérique suppose une interaction avec l'adversaire et son esprit humain, il est donc plus dynamique que les techniques basiques et passives de cybersécurité. En outre le leurrage gêne l'attaquant mais cela n'en fait toutefois pas une mesure active de cyberdéfense pour autant. En effet, comme démontré précédemment, les mesures actives de cyberdéfense sont actives du fait qu'elles soient effectuées en dehors du périmètre et qu'elles aient pour but d'avoir un effet perturbateur pour faire cesser une cyberattaque en cours. Le leurrage numérique n'a nullement ces intentions et finalités. Les artefacts de leurrage sont disposés au sein de la propre infrastructure du défenseur et n'ont absolument pas les capacités d'avoir pour effet de faire cesser les actions de l'attaquant. Au contraire, le but est soit d'attirer l'attaquant afin de collecter des informations sur ses TTP (par exemple avec un *honeypot* qui simule), soit de le gêner dans la réussite de son attaque en le trompant et le désorientant (par exemple avec un *decoy* qui dissimule). De ce fait, le leurrage numérique n'est donc pas à considérer comme une mesure active de cyberdéfense, mais bien comme une mesure passive. Toutefois, le leurrage numérique pourrait être qualifié de mesure passive proactive, alors que la mesure active est réactive. En effet, une mesure active de cyberdéfense ne doit pas être effectuée avant que la victime ait été touchée par une cyberattaque, elle en perdrait sa légitimité. Elle est une réaction, en général l'ultime recours, face à une cyberattaque qui ne pourrait pas être stoppée par d'autres moyens. Dans ce cas, c'est donc l'attaquant qui a l'initiative. A l'opposé, dans le cas du leurrage numérique, c'est le défenseur qui a l'initiative vu qu'il influence la psyché de l'individu tentant une attaque. Le défenseur ayant préparé du leurrage numérique est proactif et prend l'initiative dès qu'un adversaire interagit avec ses leurres. En conclusion, le leurrage numérique est une technique passive-proactive de cyberdéfense et le *hackback* est une mesure active-réactive de cyberdéfense.

### 4.2 La légalité du leurrage numérique au regard du droit international public

Les activités d'espionnage ne sont pas régulées par le droit international. Cela veut dire qu'elles ne sont pas illégales, toutefois en fonction de la méthode choisie elles ne sont pas non-plus légale. Le leurrage numérique peut être considéré comme des mesures de contre-espionnage et sont donc un exercice légitime du droit souverain des

Etats selon le droit international. Le leurrage numérique permet d'obtenir des indices supplémentaires afin de pouvoir déterminer qui est en train d'effectuer des actions de cyberespionnage et ces éléments peuvent ensuite être utilisés pour attribuer une cyberattaque à un Etat et prendre toutes les contre-mesures autorisées par le droit international. En outre, le leurrage numérique peut être considéré comme des ruses de guerre et est donc autorisé car ne constituant pas un acte de perfidie. Cela permet d'obtenir légalement un avantage militaire (pour le défenseur). Toutefois, la limite pourrait être dans la distinction entre les systèmes militaires et civils. Camoufler un système militaire dans un environnement civil faisant ainsi courir un risque important aux civils pourrait ne pas être autorisé. En effet, cela pourrait violer le principe d'interdiction de la perfidie voire le principe de distinction.

Dans le cas d'un *weaponised honeypot*, la question serait de savoir si cela est encore considéré comme du leurrage numérique. Nous pensons qu'il s'agit d'une zone grise qui entoure ces mesures et que cela ne peut donc pas être catégoriquement tranché. Toutefois, un système de leurrage numérique contenant des fichiers « armés » qui, une fois exfiltrés, auraient un effet perturbateur voire destructeur dans l'environnement informatiques adverse serait, selon notre définition, une mesure active de cyberdéfense et non-plus une mesure de leurrage numérique. En effet, la finalité dépasse le seuil de simplement récolter des informations sur l'attaquant, le gêner ou le désorienter. Cela pourrait avoir pour conséquence la violation de la souveraineté de l'Etat qui a exfiltré les données et ainsi subi le dommage. Malgré tout, nous imaginons mal un Etat A revendiquer des contre-mesures contre un autre Etat B car sa souveraineté aurait été violée suite à des dommages reçus en exfiltrant, lui-même, des fichiers malveillants. Il faut tout de même rappeler que, dans ce contexte, l'Etat A a pénétré en premier les réseaux de l'Etat B afin d'extraire des fichiers, même si ces derniers se sont révélés par la suite être des malicieux. L'Etat B n'a pas effectué d'action d'intrusion dans des systèmes adverses, mais seulement l'action d'installation de malicieux dans ses propres systèmes, que l'Etat A a, par accès indus et non autorisés, rapatrié chez lui. *In fine*, c'est donc l'Etat B qui pourrait revendiquer des contre-mesures envers l'Etat A pour violation de la souveraineté. En résumé, le leurrage numérique est donc légal selon notre analyse du droit international, et les quelques limites imposées sont à prendre en considération lorsqu'un Etat prépare et entend utiliser des mesures de leurrage numérique.

### 4.3 La légalité du leurrage numérique au regard du droit suisse

Le droit suisse autorise la mise en place de mesure de cybersécurité afin d'augmenter la robustesse et la résilience des systèmes informatiques garantissant ainsi un fonctionnement optimal de la société.

Premièrement, si une intrusion était détectée par une technique de leurrage numérique, le droit pénal permettrait au minimum de poursuivre les auteurs devant les tribunaux suisses pour accès indu à un système informatique voire soustraction de données.

La mise en place des mesures de leurrage numérique n'étant actuellement pas explicitement mentionnées dans les nouvelles lois de cybersécurité, elles ne sont donc pas autorisées, ni interdites. Cet état de fait pourrait changer dès que la loi sur la sécurité de l'information (LSI) entrera en vigueur. En effet, cette loi autoriserait explicitement les

services de l'Etat à user de techniques de leurrage numérique pour "améliorer leurs connaissances". Les politiques suisses étant réputés pour leur minutie et leur sens aigu du consensus, ayant pour effet de rallonger, parfois durant des années, les délais, il est actuellement impossible d'effectuer un pronostic quant à l'issue des débats parlementaires et une probable date de ratification de la LSI. En outre le droit de référendum pourrait encore prolonger la date d'entrée en vigueur de la LSI. Dans un autre registre, une nouvelle étape a été franchie avec la création du NCSC en été 2020 et l'entrée en vigueur de l'ordonnance sur la protection contre les cyberrisques dans l'administration fédérale (OPCy). Cette ordonnance donne de nouvelles prérogatives aux services étatiques chargés de la cybersécurité et du soutien aux infrastructures critiques. En particulier, les questions de respect de la vie privée et de protection des données ont été clarifiées. Les services de l'Etat ont maintenant un intérêt légitime à traiter des données personnelles, même à l'insu des personnes concernées, si elles sont utiles à la cybersécurité. En outre un délai maximal de conservation de cinq ans a été fixé. La question de l'échange transfrontalier des données est également autorisé pour la cybersécurité des infrastructures critiques.

Sachant que le leurrage numérique n'est pas considéré comme une mesure active de cyberdéfense, les lois sur le renseignement (LRens) et sur l'armée (LAAM) ne s'applique pas. En tout cas pas si ces mesures sont mises en œuvre sur le territoire suisse. Toutefois, si une mesure de leurrage numérique devait être mise en place à l'étranger, que cela soit en terrain neutre ou en terrain adverse, ces lois pourraient s'appliquer. Cela serait également le cas d'un *weaponised honeypot* installé en Suisse, car cela pourrait impliquer une pénétration dans des réseaux informatiques à l'étranger. Les conditions requises (la cible attaquée doit être en Suisse, être une infrastructure critique et la cyberattaque doit provenir de systèmes et réseaux se trouvant à l'étranger) doivent être remplies et une demande devrait être formulée au gouvernement fédéral, fournissant toutes les indications requises par les ordonnances (ORens et OCMil). *In fine*, c'est le Conseil fédéral qui déciderait de la mise en œuvre de ces mesures et qui porterait la responsabilité politique de l'autorisation de telles mesures qui pourraient être considérées, par les Etats étrangers, comme une violation de leur souveraineté, les légitimant à prendre des contre-mesures envers la Suisse.

En résumé, le cadre légal helvétique de cybersécurité est en train d'évoluer, ces dernières années, dans une direction plutôt autorisante pour les services étatiques fédéraux. Bien que ces services aient les bases légales pour effectuer de nombreuses actions dans le cyberspace, plusieurs garde-fous ont été mis en place afin d'empêcher des dérives. En particulier une claire répartition des rôles et responsabilités garantissent une séparation des pouvoirs. Bien qu'on remarque une tendance à la centralisation au niveau fédéral des compétences, elles sont réparties au sein de plusieurs unités qui sont disséminées au sein de plusieurs départements fédéraux. Ainsi, pour mettre en œuvre une mesure, il y aura toujours plusieurs unités voire départements impliqués et le risque de dérapage est donc limité. Enfin, de nombreux organismes de contrôles, qu'ils soient exécutifs, législatifs ou juridiques, ont été mis en place. Toutes ces mesures devraient permettre d'encadrer la pratique du leurrage numérique en Suisse.

## 5 Conclusion

Que cela soit dans le monde animal ou militaire, le leurrage est une technique de déception qui existe depuis plusieurs siècles. Il repose sur deux concepts fondamentaux à savoir montrer le faux "la simulation" et cacher le vrai "la dissimulation". Le leurrage numérique tire profit de ces principes et les imite dans le domaine informatique, par des outils comme le *honeypots* qui simule ou le *decoy* qui dissimule, afin de donner un avantage au défenseur et rendre la tâche de l'attaquant plus ardue. Ce concept n'a fait l'objet que récemment de formalisation et de mesure d'accompagnement et d'encadrement. De nombreuses zones grises sont encore présentes tant dans le domaine de la définition de sa taxonomie que dans les cadres légaux le régulant. Juridiquement, il ne semble pas interdit mais ne nécessite pas non plus d'autorisation explicite. C'est peut-être du fait qu'il soit considéré comme inoffensif par une majorité, qu'il n'a pas fait, actuellement, l'objet de plus d'attention que nécessaire. Historiquement, on remarque que le leurrage repose essentiellement sur l'interaction entre humains. Il s'agit d'un jeu où chacun tente de jouer son coup et de surprendre l'autre pour obtenir un avantage. Une opération de leurrage numérique consiste en une planification, un développement et un déploiement d'un ensemble d'actes pour induire en erreur l'attaquant et l'inciter à effectuer une action ou une inaction qui favorise la cybersécurité (Yuill et al., 2006). Le but de ces actions de leurrage numérique est d'inciter l'attaquant à opter pour un comportement prévisible qui peut être exploité par le défenseur (Heckmann et al., 2013). Dans ce domaine il est intéressant de relever que deux mondes semblent s'opposer : les praticiens de la cybersécurité, personnes majoritairement issues du domaine technique, et les praticiens de la cybersécurité qui sont en majorité composés de personnes issues du domaine sécuritaire ou militaire. En effet, les premiers ont comme objectifs principaux d'éviter l'intrusion par tous les moyens et, si un incident venait à se produire, de le régler au plus vite en rétablissant le service affecté à la normale dans les plus brefs délais. Ainsi, dans ce contexte de cyberprotection, des mesures de leurrage numérique pourraient être considérées comme des mesures architecturales de cybersécurité et n'avoir qu'une efficacité passive en servant uniquement de détecteurs d'intrusion. Rajoutant ainsi une simple couche supplémentaire tel que décrit dans le concept de défense en profondeur (*defense in depth*). A l'opposé, les seconds partent du principe que l'intrusion fait partie des possibilités dont il faut profiter des opportunités pour se renseigner sur l'attaquant afin de comprendre sa technique d'attaque et de mieux pouvoir réagir et de s'en prémunir, voire de jouer un peu avec lui (efficacité active). Par ailleurs, est-ce que le leurre numérique pourrait être utilisé, sous certaines conditions, dans le cadre d'une stratégie A2/AD (*Anti-access, Area Denial*), soit comme une technique de déni d'accès et d'interdiction de zone ?

Il sera intéressant d'observer si, à l'avenir, avec l'automatisation et l'utilisation de l'intelligence artificielle dans des cyberattaques ces techniques de leurre auront encore les mêmes chances de succès et garderons ainsi un si grand intérêt. En outre, la tendance à l'armement des techniques de leurrage pour les rendre plus réactives, plus rapides et plus perturbantes pourrait déboucher, un jour, sur un incident aux conséquences imprévues mais potentiellement néfastes, par exemple des dégâts collatéraux non contrôlés ou des ripostes immédiates et automatique sur de mauvaises cibles. Mais n'est-ce pas

le risque encouru par le développement des capacités dans le cyberspace couplé à l'augmentation de l'interconnectivité et de l'automatisation de plus en plus de systèmes de nos sociétés modernes ? Le rôle du régulateur pourrait encore plus s'affirmer, réjouissant certains et mécontentant les autres. C'est un clivage technico-libéraliste – juridico-étatique.

## Références

1. Administration fédérale Suisse (2014), Rapport explicatif sur le projet de loi sur la sécurité de l'information du 26 mars 2014. Berne, Suisse. Extrait à : [https://www.admin.ch/ch/f/gg/pc/documents/2279/LSI\\_Rapport-expl\\_fr.pdf](https://www.admin.ch/ch/f/gg/pc/documents/2279/LSI_Rapport-expl_fr.pdf)
2. Assemblée fédérale Suisse. (2020). Loi fédérale sur l'armée et l'administration militaire (LAAM). Berne, Suisse. Extrait de <https://www.admin.ch/opc/fr/classified-compilation/19950010/index.html>
3. Assemblée fédérale Suisse. (2020). Loi fédérale sur le renseignement (LRens). Berne, Switzerland. Extrait de <https://www.admin.ch/opc/en/classified-compilation/20120872/index.html>
4. Barel, M. (2004). « Honey pots : un pot-pourri. . . juridique » - SSTIC 2004, actes de la conférence
5. Bell, J. B., & Whaley, B. (1991). *Cheating and deception*. Transaction Publishers.
6. Brandt, A., & Wolff, Z. (2010). When admins attack: 30 hours in the life of a Gumblar victim. *Network Security*, 2010(2), 4-8.
7. Bringer, M. L., Chelmecki, C. A., & Fujinoki, H. (2012). A survey: Recent advances and future trends in honeypot research. *International Journal of Computer Network and Information Security*, 4(10), 63.
8. Chakravarty, S., Portokalidis, G., Polychronakis, M., & Keromytis, A. D. (2011, September). Detecting traffic snooping in tor using decoys. In *International Workshop on Recent Advances in Intrusion Detection* (pp. 222-241). Springer, Berlin, Heidelberg.
9. Conseil fédéral Suisse. (2017). Ordonnance sur le service de renseignement (ORens). Berne, Suisse. Extrait de <https://www.admin.ch/opc/fr/classified-compilation/20162430/index.html>
10. Conseil fédéral Suisse. (2020). Ordonnance sur la cyberdéfense militaire (OCMil). Berne, Suisse. Extrait de <https://www.admin.ch/opc/fr/classified-compilation/20182319/index.html>
11. Conseil fédéral Suisse. (2020). Ordonnance sur la protection contre les cyberrisques (Ord-PCy). Berne, Suisse. Extrait de <https://www.admin.ch/opc/fr/classified-compilation/20200291/index.html>
12. De Faveri, Cristiano, Ana Moreira, and Vasco Amaral. "Multi-paradigm deception modeling for cyber defense." *Journal of Systems and Software* 141 (2018): 32-51.
13. Denning, D. E., & Strawser, B. J. (2014). Active cyber defense: Applying air defense to the cyber domain. *Cyber Analogies*. Calhoun: The National Postgraduate School (NPS) Institutional Archive.
14. Département fédéral de la défense, de la protection de la population et des sports (DDPS), (2017), Loi fédérale sur la sécurité de l'information au sein de la Confédération (LSI). Berne, Suisse. Extrait de <https://www.vbs.admin.ch/fr/themes/securite-information/loi-securite-information.detail.document.html/vbs-internet/fr/documents/lsi/LSI.pdf.html>
15. Dewar, R. S. (2017). Active Cyber Defense. *CSS Cyber Defence Trend Analysis*, 1.
16. Dulles, A. W. (1964). *The craft of intelligence*. Harper & Row.

17. Ferguson-Walter, K & LaFon, D 2015, 'Deception for cyber defense: a case study', *Journal of Sensitive Cyber Research and Engineering*, vol. 3, no. 1, pp. 45-58.
18. Ferguson-Walter, Kimberly J., Dana S. LaFon, and T. B. Shade. "Friend or faux: deception for cyber defense." *Journal of Information Warfare* 16.2 (2017): 28-42.
19. Ghernaoui, S. (2013). *Cyber power: Crime, Conflict and Security in cyberspace*. EPFL Press, CRC Press
20. Heckman, Kristin E., et al. "Active cyber defense with denial and deception: A cyber-war-game experiment." *computers & security* 37 (2013): 72-77.
21. Hilbert, M. (2012). Toward a synthesis of cognitive biases: how noisy information processing can bias human decision making. *Psychological bulletin*, 138(2), 211.
22. Iasiello, E. (2014). Hacking back: Not the right solution. *Parameters*, 44(3), 105.
23. Kello, L. (2016). Private-Sector Cyberweapons: Strategic and Other Consequences. *Available at SSRN 2836196*.
24. Ormrod, D. (2014, October). The coordination of cyber and kinetic deception for operational effect: attacking the C4ISR interface. In *2014 IEEE Military Communications Conference* (pp. 117-122). IEEE.
25. OTAN, Bureau OTAN De Normalisation (NSO). 2019. AAP-06 (2019) – Glossaire OTAN de termes et définitions (anglais et français).
26. Provos, N. (2004, August). A Virtual Honeypot Framework. In *USENIX Security Symposium* (Vol. 173, No. 2004, pp. 1-14).
27. Qassrawi, M. T., & Hongli, Z. (2010, April). Deception methodology in virtual honeypots. In *2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing* (Vol. 2, pp. 462-467). IEEE.
28. Rosenzweig, P. (2014). International law and private actor active cyber defensive measures. *Stan. J. Int'l L.*, 50, 103.
29. Rosenzweig, P., Bucci, S. P., & Inserra, D. (2017). Next Steps for US Cybersecurity in the Trump Administration: Active Cyber Defense. *Backgrounders*, (3188), 11.
30. Rowe, N. C., Custy, E. J., & Duong, B. T. (2007). Defending cyberspace with fake honeypots. *JCP*, 2(2), 25-36.
31. Rowe, N. C., Duong, B. T., & Custy, E. J. (2006, June). Fake honeypots: A defensive tactic for cyberspace. In *Proc. of the IEEE Workshop on Information Assurance* (pp. 223-230).
32. Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.
33. Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.
34. Smith, D. L. (2005). Why We Lie. The Evolutionary Roots of Deception and the Unconscious Mind.
35. Sokol, P., Míšek, J., & Husák, M. (2017). Honeypots and honeynets: issues of privacy. *EURASIP Journal on Information Security*, 2017(1), 1-9.
36. Spitzer, L. (2003): Honeypots: Are They Illegal?. Broadcom Endpoint Protection. Extrait de <https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=5a410cac-a00c-4204-bd2c-544cff6f391f&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments>
37. Spitzner, L. (2003). *Honeypots: tracking hackers* (Vol. 1). Reading: Addison-Wesley.
38. Spitzner, L. (2003). Honeytokens: The other honeypot.
39. Spitzner, L. (2003). The honeynet project: Trapping the hackers. *IEEE Security & Privacy*, 1(2), 15-23.

40. Unité de pilotage Informatique de la confédération (UPIC). (2012). Stratégie nationale de protection contre les cyberrisques 2012-2017. Berne, Suisse. Extrait de [https://www.isb.admin.ch/isb/en/home/themen/cyber\\_risiken\\_ncs/ncs\\_strategie-2012.html](https://www.isb.admin.ch/isb/en/home/themen/cyber_risiken_ncs/ncs_strategie-2012.html)
41. Unité de pilotage Informatique de la confédération (UPIC). (2018). Stratégie nationale de protection contre les cyberrisques 2018-2020. Berne, Suisse. Extrait de [https://www.isb.admin.ch/isb/en/home/themen/cyber\\_risiken\\_ncs/ncs\\_strategie.html](https://www.isb.admin.ch/isb/en/home/themen/cyber_risiken_ncs/ncs_strategie.html)
42. Vrabie, M., Ma, J., Chen, J., Moore, D., Vandekieft, E., Snoeren, A. C., ... & Savage, S. (2005, October). Scalability, fidelity, and containment in the potemkin virtual honeyfarm. In *Proceedings of the twentieth ACM symposium on Operating systems principles* (pp. 148-162).
43. Wanner, B., & Ghernaoui, S. (2019). Conceptualizing Active Cyber Defence in Cyber Operations: Quo Vadis, Switzerland?. *St Antony's International Review*, 15(1), 58-82.
44. Wanner, B., & Ghernaoui, S. (2020). Active Defensive Measures in Cyberspace – a Swiss Case Study. *European Cybersecurity Journal*, Volume 6 (2020) Issue 2, 79-90.
45. Whaley, B. (1969). *Stratagem: deception and surprise in war*. Cambridge, Mass.: Center for International Studies, Massachusetts Institute of Technology, c1969.
46. Yuill, J., Denning, D., & Feer, F. (2006). Using deception to hide things de hackers: Processes, principles, and techniques. *Journal of Information Warfare*, 5(3), 26-40.