NOTE À BON DE COMMANDE N° 6

Note n° 166/Consortium OBSAT-35
du 2 novembre 2020

Marché n° 2017 1050 100 589
notifié le 9 octobre 2017
Tranche 3 – réunion de lancement : 21 octobre 2019

Bon de commande n° 6 – Référence n° 140 508 80 38
notifié le 7 juillet 2020

Quels seraient les impacts d'une pandémie numérique pour l'armée de Terre
(fonctionnement et rôle au sein de la Nation) ?

THIBAULT FOUILLET – BRUNO LASSALLE

EUROCRISE
Agence d'Intelligence Stratégique

FONDATION pour la RECHERCHE STRATÉGIQUE

WWW.FRSTRATEGIE.ORG | 4 BIS RUE DES PATURES 75016 PARIS | TEL : 01.43.13.77.77 | MAIL : CONTACT@FRSTRATEGIE.FR
SIRET 39409553300052 TVA FR74 394 095 533 CODE APE 7220Z FONDATION RECONNUE D'UTILITÉ PUBLIQUE DÉCRET DU 26 FÉVRIER 1993
WWW.EUROCRISE.COM | 8 RUE DE BELLEFOND 75009 PARIS | TEL : 01.49.49.01.23 | MAIL : EUROCRISE@EUROCRISE.COM
SIRET 438 431 207 00036 TVA FR 1743 8431 2070 0036 COPE APE 7022Z

SOMMAIRE

SYNTHÈSE **1**

INTRODUCTION **3**

1. QUELLES MENACES POUR L'ARMÉE DE TERRE POUR QUELLES PANDÉMIES NUMÉRIQUES ? **6**

1.1. De la pandémie numérique : essais de définition **6**

1.1.1. La cause cyber 7

A. Le modèle en kill chain 7

B. L'hypothèse d'un dommage collatéral 9

1.1.2. La cause non-cyber à effets équivalents 11

1.1.3. L'hypothèse accidentelle ou par cause naturelle 12

1.2. La place de l'armée de Terre en cas de pandémie numérique : un usage fortement encadré de l'outil militaire **14**

1.2.1. L'action de l'armée de Terre, un rôle secondaire 14

1.2.2. Une fonction d'assistance consacrée par le droit 16

2. QUELLES ACTIONS POUR L'ARMÉE DE TERRE EN CAS DE DEMANDE DE CONCOURS POUR FAIRE FACE À UNE PANDÉMIE NUMÉRIQUE ? **18**

2.1. Des missions générales armée de Terre pour parer aux dysfonctionnements collatéraux engendrés par la pandémie numérique **18**

2.1.1. Cadre de l'action 18

2.1.2. Esquisse des missions 19

2.2. Les actions spécialisées dans le numérique menées par l'armée de Terre pour parer sur le coup aux dysfonctionnements directs engendrés par la pandémie sur les systèmes et réseaux d'information **20**

2.2.1. Capacités 20

2.2.2. Esquisse des missions 21

3. QUELLE RÉSILIENCE PROPRE À L'ARMÉE DE TERRE DANS LE CADRE DU SCÉNARIO « PANDÉMIE NUMÉRIQUE » ? **24**

3.1. L'impact d'une pandémie numérique sur les forces terrestres : résilience et vulnérabilités **24**

3.1.1. Étude des conséquences probables sur les capacités de l'armée de Terre 24

3.1.2. Des capacités de résilience de l'armée de Terre face à une pandémie numérique civile 27
A. Le mode dégradé, une solution de court terme 27
B. L'apport de l'armée de Terre face à une pandémie numérique : des moyens limités 28
3.2. Développer les capacités de résilience numérique à horizon 2035 29
3.2.1. Comment les grandes puissances envisagent-elles un renforcement de leur résilience numérique ? 30
3.2.2. Développer les capacités de résilience numérique de l'armée de Terre 32
CONCLUSION 35

Synthèse

La pandémie numérique est un sujet qui n'a pas fait l'objet d'une véritable documentation. L'occurrence d'un tel phénomène qui dépasserait une simple panne pour intéresser de vastes zones durant une période importante, est souvent considérée comme faible, au point de la négliger voire de la classer arbitrairement dans la catégorie des fantasmes. Mais comme en toute chose, la capacité à anticiper une crise peut faciliter son traitement et accélérer le retour à la normale.

En effet, un effondrement localisé et durable de l'internet peut se trouver lié à des causes naturelles spécifiques de grande ampleur, accidentelles du fait de la défaillance d'installations techniques, ou intentionnelles du fait d'actes malveillants terroristes ou de guerre. La robustesse du réseau de communication maillé que nous connaissons peut-être mise à défaut par des pannes généralisées d'électricité ou la destruction simultanée de composants électroniques uniformément répartis dont la fragilité ou la vulnérabilité à des actions spécifiques n'avaient pas été détectées.

Les impacts sur la vie de la nation seraient majeurs du fait de la généralisation des applications internet qui pilotent aujourd'hui la presque totalité des réseaux utilisés par les administrations, les particuliers ou les industriels. Ainsi, le dysfonctionnement de l'internet aurait un effet domino sur les réseaux de transport d'énergie (électricité, gaz, oléoducs), de transport ferroviaire et dans une moindre mesure aujourd'hui routière, télécommunications (particuliers, banques…). En conséquence le pays serait frappé d'une certaine paralysie entraînant des désordres importants dictés par les tentatives de survie face aux différents blocages. La situation de 2035 serait encore plus difficile à gérer que celle d'aujourd'hui du fait de la multiplication des objets connectés.

Dans ce cadre, les forces armées et l'armée de Terre en particulier peuvent être réquisitionnées pour intervenir et les missions qui en découlent doivent être imaginées dans le cadre d'une démarche générale d'anticipation qui ne vise pas nécessairement le retour à la normale, mais la stabilisation dans un état acceptable dans une logique de résilience.

Deux types de missions peuvent être envisagés sous forme de réquisition conformément aux conventions existantes, en utilisant les structures de commandement des zones de défense. D'une part des missions de sécurité civiles permettant dans l'urgence de renforcer le service public en apportant le concours d'hommes et de matériels. D'autre part des missions proprement militaires pour protéger les points d'importance vitale dont les systèmes de sécurité seraient devenus inopérants. Enfin, des missions principalement techniques pour rétablir les

moyens de communication en utilisant des réseaux militaires pour une grande part indépendants de l'internet.

Des enseignements et recommandations viennent conclure la note, en insistant sur l'importance de l'acceptabilité du temps de retour à la normale et notamment du service dégradé qu'il s'agirait de mettre sur pied. Parmi ces enseignements, certains seront dédiés aux évolutions de la réserve pour que celle-ci soit au mieux adaptée à ces missions nouvelles.

Quels seraient les impacts d'une pandémie numérique pour l'armée de Terre (fonctionnement et rôle au sein de la Nation) ?

Introduction

La pandémie de la Covid-19 toujours en cours a surpris par sa soudaineté et sa capacité à paralyser l'entièreté du fonctionnement de la nation, réactualisant les concepts de surprise stratégique et de résilience. Dans ce cadre, une étude des crises similaires possibles pouvant affecter l'armée de Terre de manière directe ou indirecte (en tant que soutien aux organes civils de l'État) semble nécessaire. À ce titre, le cadre d'une pandémie numérique est le plus emblématique. En effet, la soudaineté d'une attaque ou d'un accident numérique, leurs caractères protéiformes, et leurs impacts pouvant être aussi bien ciblés que généraux, renvoient peu ou prou au cadre pandémique.

▶ La 'pandémie numérique' pour l'armée de Terre de quoi s'agit-il ?

Les forces terrestres ont eu dans le cadre de la crise sanitaire à jouer un rôle de soutien en mettant à disposition leurs éléments spécialisés pour assister les moyens civils de résilience. Bien qu'une logique similaire puisse opérer dans le cadre d'une pandémie numérique, sa possible origine malveillante pourra en outre attaquer directement des éléments de l'armée de Terre impliquant une réaction adaptée en fonction de la menace.

En effet, lors d'une pandémie, un agent pathogène peut attaquer un organe ou une fonction d'un organisme humain, sa destination et les méfaits engendrés permettant de le classer et de le nommer. Par analogie, dans le cadre d'une pandémie numérique, tout système d'armes ou fonction militaire utilisant des informations numérisées est susceptible de constituer la cible d'une attaque spécifique qu'il faut savoir détecter puis identifier, avant de la combattre avec réactivité et l'anticiper à l'avenir en s'en protégeant.

De ce fait, pour bien comprendre le niveau de vulnérabilité de l'armée de Terre dans ce nouveau champ d'action au carrefour de l'électronique et de l'informatique, il faut examiner tous les aspects de la défense terrestre qui tirent parti des applications numériques en identifiant de manière exhaustive les vulnérabilités.

De ce fait, trois éléments principaux posent question dans la réalisation de cette note :

Sous quelle forme peut s'incarner la pandémie numérique ? Impliquant par ailleurs de déterminer en fonction des divers scénarios de paralysie des systèmes, quels éléments des forces terrestres seraient impactés et/ou mobilisés ?

Quel serait l'impact d'une pandémie numérique générale, autrement dit universelle (à l'instar de la Covid au plan sanitaire) sur le fonctionnement des forces terrestres, et quel rôle pourraient-elles jouer dans l'assistance aux moyens civils pour assurer la résilience de la nation ?

En cas d'attaque ciblée sur les forces terrestres par un ennemi recherchant un avantage opérationnel par la paralysie des moyens numériques sur un théâtre d'engagement, quel serait l'impact probable sur l'armée de Terre ? Quels seraient les parades et les moyens de garantir une résilience ?

Bien qu'importante, la troisième interrogation concernant l'impact d'une attaque numérique sur les forces en opérations constitue en elle-même un sujet à part entière. Or, eu égard au format court de ce document de recherche dont le cœur de cible est constitué par une pandémie numérique civile contre laquelle l'armée agirait en soutien, la dimension des opérations extérieures ne sera pas traitée ici.

- **Pour l'armée de Terre, il s'agit de caractériser la menace et son rôle dans cette crise civile afin d'en déduire les conséquences sur ses moyens**

À la lumière de ces éléments de contextualisation, cette note vise à caractériser la pandémie numérique et le rôle de l'armée de Terre dans sa résolution, elle ambitionne également de définir les impacts directs et indirects de ce type de pandémie sur les forces terrestres afin d'en dégager des vulnérabilités et finalement déduire un ensemble de recommandations salvatrices.

Par conséquent le plan d'étude suit une organisation en trois parties :

- **Étape 1 : Quelles pandémies numériques pour quelle place de l'armée de Terre ?**

Comme toute étude d'anticipation, une analyse de l'impact d'une 'pandémie numérique' implique de définir les diverses manifestations de la menace et de ses effets prévisibles avant de pouvoir en tirer des conséquences sur le rôle des armées et leurs vulnérabilités éventuelles.

Par conséquent, l'objectif de cette étape réside dans une définition de la pandémie numérique et de ses contours probables d'apparition, pour pouvoir en déduire les effets attendus sur la société civile. Par la suite, en prenant en compte ces éléments, le rôle de l'armée de Terre pourra être défini (direct, indirect, accessoire, primordial…), préalable indispensable à une étude détaillée de ses actions et capacités garantissant la résilience.

➡ **Étape 2 : Quelles actions pour l'armée de Terre afin de contribuer à la résilience de la nation face à une pandémie numérique ?**

Une fois défini le contour de la menace et précisé la place de l'armée de Terre dans une lutte contre une pandémie numérique civile déterminée, il conviendra d'effectuer une analyse détaillée de l'action des forces terrestres. Bien que partie moins conséquente en volume que les autres étapes puisque plus spécialisée, l'enjeu de cette partie est central en permettant de déterminer la capacité de l'armée de Terre à contribuer à la résilience de la nation et l'ampleur de son rôle dans celle-ci.

➡ **Étape 3 : Étude de la résilience propre à l'armée de Terre face à des perturbations numériques massives**

Enfin, après l'étude de la menace, et la compréhension de l'action concrète de l'armée de Terre dans la lutte contre une pandémie numérique compromettant la résilience de la nation, il sera temps de déterminer l'impact d'une telle crise sur les moyens propres à l'armée de Terre, ainsi que sur sa capacité à agir en soutien des organes civils. Cœur de cette étude, cette partie aura pour enjeu de dégager les vulnérabilités probables de l'appareil de forces dans un tel contexte, et par une étude des parades envisagées (y compris par une analyse des programmes des autres puissances en la matière), de présenter un ensemble de recommandations formulées selon la classification DORESE.

1. Quelles menaces pour l'armée de Terre pour quelles pandémies numériques ?

En 2020, suite à la quasi-paralysie du système économique international due à la pandémie provoquée par la COVID-19, le monde s'apprête à entrer dans une récession économique forte. Au-delà de cet impact de court/moyen terme, d'autres effets ont été constatés, sur le plan politique suite à l'impréparation à plusieurs niveaux (OMS, Union européenne, États européens, etc.), mais également environnemental avec une amélioration de la situation globale due à la baisse des émissions de gaz à effet de serre. Même si certaines conséquences ne s'avèrent pas négatives, la pandémie de COVID-19 est dans son ensemble un défi sanitaire, économique et politique majeur pour l'ensemble des organisations de la planète.

De manière comparable à cette situation, il est nécessaire d'évaluer aujourd'hui les évènements qui pourraient provoquer une paralysie de grande ampleur de type numérique envisagée en tant que disruption profonde – dans le temps et dans l'espace – de l'accès aux services numériques.

Ces derniers sont en effet devenus des socles de nos vies, aussi bien que de nos activités professionnelles, par l'accélération de l'interconnexion. Le domaine militaire n'échappe pas à ce phénomène, avec un recours toujours plus poussé aux équipements numériques, dans et hors du champ de bataille.

Il convient ainsi d'évaluer les conditions de l'apparition d'une « pandémie numérique » et ses conséquences afin d'envisager le rôle de l'armée de Terre française dans sa résolution.

1.1. De la pandémie numérique : essais de définition

Une pandémie numérique, entendue de manière générique dans le sens d'une paralysie profonde et continue de l'accès aux services numériques, ne constitue pas un concept homogène. En effet, des causes multiples peuvent être à l'origine d'une perturbation des moyens numériques, entraînant des conséquences plus ou moins pérennes et graves pour la société civile.

Bien que l'objet de cette note de recherche ne soit pas l'étude de cette pandémie mais bien de son impact, l'on ne peut s'affranchir d'une analyse des causes, puisque celle-ci permettra de caractériser de manière concrète les effets probables sur la société et sur l'armée de Terre. Par conséquent, c'est uniquement par ce biais que l'on pourra envisager le rôle que cette dernière aura à tenir ainsi que l'impact de la rupture numérique sur son fonctionnement.

La pandémie numérique apparaît ainsi comme pouvant émerger de trois sources principales : la première est le lancement d'une attaque cyber de grande ampleur, touchant des systèmes particulièrement répandus ; la seconde est le déni d'accès aux communications électroniques par paralysie électromagnétique et attaque des éléments physiques de communication ; la troisième étant le scénario d'une pandémie numérique suite à un accident de grande ampleur ou une catastrophe naturelle.

1.1.1. La cause cyber

Une action issue du champ cyber représente le scénario le plus emblématique et le plus probable de déclenchement d'une pandémie numérique, étant donné les antécédents déjà observés depuis plus d'une décennie. Une pandémie numérique suppose ici une action – considérée dans ce contexte comme intentionnelle ou quasi-intentionnelle[1] – maligne envers un système numérique donné. Les deux alternatives décrites ci-dessous posent avant tout la question de l'utilisation dans le contexte militaire de matériels civils ou duaux, autant sur le *hardware* (ordinateurs et structures filaires) ou le software (logiciels).

La difficulté, voire dans certains cas l'impossibilité, d'avoir recours à des éléments spécifiquement militaires de bout en bout renforce l'hypothèse d'une pandémie se propageant depuis le domaine civil. Deux modèles pratiques de cette pandémie par cause cyber sont possibles : une logique en *kill chain* ou une hypothèse collatérale.

A. Le modèle en kill chain

L'hypothèse d'une attaque intentionnelle spécifique sur certains systèmes est celle qui porte le plus de craintes. Depuis le vol et la diffusion – limitée jusqu'ici – des outils cyber-offensifs de la NSA par le groupe *The Shadow Brokers*[2], des actions offensives particulièrement dangereuses ont été observées. Les outils développés pour la branche cyber-offensive de la NSA, le *Tailored Access Operations*, comprenaient entre autres une série de failles inconnues – dites *zero day* – dans des systèmes particulièrement répandus. Il s'agit notamment de la faille EternalBlue[3] dans les logiciels OS Microsoft qui a ensuite été exploitée par des groupes criminels, « hacktivistes » ou étatiques pour développer des maliciels spécifiques : WannaCry dans un premier temps, puis NotPetya (2017).

Ces deux attaques ont mis en avant le modèle de mise en œuvre des cyberattaques dit de *kill chain* qui repose sur une succession d'étapes afin d'obtenir un résultat maximal. Si WannaCry pouvait encore être considéré comme une action conventionnelle de type cybercriminel, NotPetya qui lui succède quelques mois plus tard est une action de niveau étatique ou militaire, clairement destinée à détruire des systèmes entiers. NotPetya prend ainsi l'aspect d'un *ransomware* déjà connu (Petya) mais camoufle sous cette apparence un système de verrouillage (*cryptolocker*) et d'effacement (*wiper*) des fichiers de la machine infectée[4]. Ces deux attaques

---

[1] L'un des grands défis des actions dans le cyberespace, en particulier la dissémination de maliciels, est l'incapacité à en contrôler les effets dans le temps et l'espace. Le cas du ver Stuxnet est ici parlant puisque celui-ci avait été conçu spécifiquement pour viser une vulnérabilité particulière dans le système de contrôle des centrifugeuses du centre nucléaire de Natanz en Iran. Ce système étant déconnecté du réseau Internet, Stuxnet y a probablement été introduit par une complicité interne – suivant le concept des attaques dites « cyber-physiques » – toutefois il aurait ensuite été téléchargé par erreur par un employé qui, une fois le matériel infecté – clé USB ? – relié au réseau Internet, a répandu Stuxnet bien au-delà des frontières iraniennes. On estime ainsi à environ 200 000 le nombre de machines infectées dans le monde.

[2] Dont l'identité demeure pour l'instant sujette à spéculations.

[3] Bill Fassinou, « EternalBlue, un outil de piratage de la NSA volé par des pirates, fait des ravages », securite.developpez.com, 26 mai 2019 – https://securite.developpez.com/actu/263137/EternalBlue-un-outil-de-piratage-de-la-NSA-vole-par-les-pirates-fait-des-ravages-causant-des-milliards-de-dollars-de-dommages/.

[4] Ellen Nakashima, « Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes », whashingtonpost.com, 13 janvier 2018 – https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html.

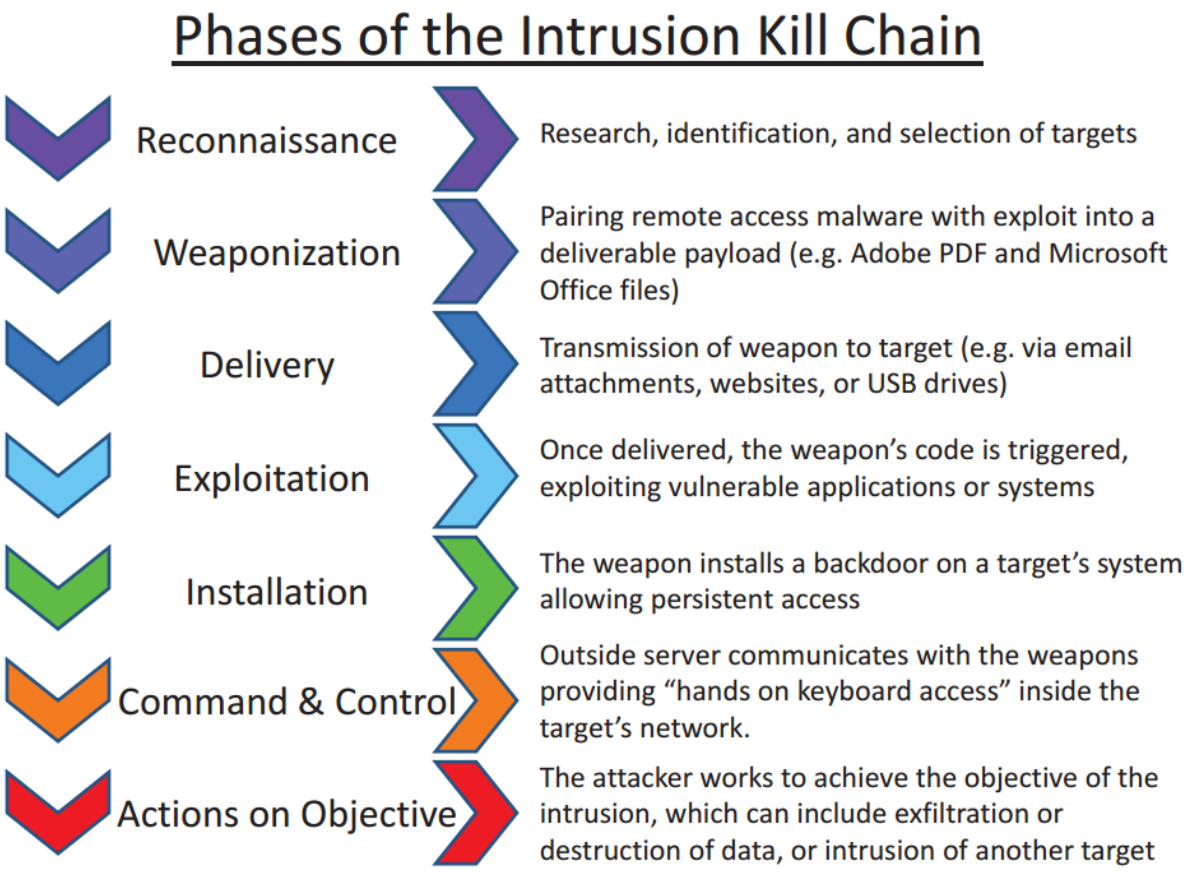
qui ont visé le territoire ukrainien, ont eu des conséquences importantes à la fois en Ukraine (atteinte de systèmes liés au réseau électrique) mais également au-delà (propagation internationale à partir des filiales ukrainiennes d'entreprises transnationales)[5]. *In fine*, les auteurs de WannaCry et NotPetya ne sont pas identifiés formellement.

Toutefois, un certain nombre d'analyses forensiques américaines, canadiennes et australiennes les relient – pour NotPetya en particulier – aux services de renseignement russes, au travers du groupe connu sous le nom de *Sandworm*.

Il s'agit ici d'une action conduite par un groupe structuré qui met en œuvre un processus complexe de renseignement – y compris dans la phase de recherche de vulnérabilité *zero day* –, élaboration de l'arme, dissémination, contrôle de l'efficacité qui se révèle d'autant plus dangereux que la faille identifiée l'est dans un système particulièrement populaire.

Le schéma ci-dessous explicite les phases d'une attaque de *kill chain*[6] *:*

Figure n° 1 : MODÈLE DE *KILL CHAIN*



[5] The Guardian, « US join UK in blaming Russia for NotPetya cyber-attack », theguardian.com, 15 février 2018 – https://www.theguardian.com/technology/2018/feb/15/uk-blames-russia-notpetya-cyber-attack-ukraine.

[6] Sarah Hosphelhorn, « What is The Cyber Kill Chain and How to Use it Effectively », varonis.com, 29 mars 2020 – https://www.varonis.com/blog/cyber-kill-chain/#:~:text=.

Au-delà de ces attaques sur les systèmes logiciels, d'autres vulnérabilités majeures ont été découvertes ces dernières années sur les systèmes matériels, notamment sur certains types de processeurs. Il s'agit en particulier des vulnérabilités Meltdown et Spectre (2018)[7]. Ce sont des vulnérabilités au sein des micrologiciels de processeurs à haute capacité (x64 et x86), dont certains d'entre eux pourraient être utilisés pour des applications liées à l'intelligence artificielle (IA). Une attaque sur micrologiciel est d'autant plus complexe à contrer que ceux-ci sont plus difficiles à mettre à jour que des logiciels conventionnels. L'exposition des systèmes informatiques, en particulier militaires, aux vulnérabilités des micrologiciels va mécaniquement augmenter par l'introduction de plus en plus d'objets connectés destinés à la numérisation de l'espace de bataille.

Dans le cas du développement d'applications militaires dédiées sur des appareils civils, comme c'est le cas pour le système Auxylium par exemple, ce type de vulnérabilité représente un risque majeur, en offrant un accès au système par son cœur matériel.

Le champ de ces menaces en *kill chain* étant avant tout centré sur une attaque ciblée de la part d'un État ou d'un groupe structuré aurait tendance *a priori* à cantonner l'action numérique à un effet localisé sur un groupe particulier (par exemple les forces armées).

Toutefois deux éléments permettent d'envisager la *kill chain* comme cause d'une pandémie numérique :

- **La contagion** : ici le cas ukrainien présenté précédemment est significatif. En effet l'interconnexion des entreprises et des entités gouvernementales impliquera bien souvent qu'une attaque sur un organisme aura des répercussions sur d'autres, pour au final une paralysie par propagation du virus (à l'image d'une pandémie sanitaire).
- **L'attaque sur des systèmes vitaux** : il s'agit du scénario le plus catastrophique avec une attaque sur les serveurs civils organisant l'énergie ou les transports et pouvant directement causer des victimes ainsi qu'une situation chaotique.

Dans les deux cas, les effets sur la société seront à l'origine localisés puisque l'attaque en *kill chain* s'effectue sur une cible déterminée, pour par la suite se développer progressivement à l'ensemble de la société avec pour objectif de déclencher une panique généralisée qui ne pourra être endiguée du fait d'une paralysie des moyens numériques de l'État et donc un ralentissement de leurs capacités d'action. L'effet de contagion accentuant la pression psychologique par un effet produit d'inéluctabilité du phénomène et de l'incapacité de l'État à réagir, comme pour une pandémie sanitaire.

B. L'hypothèse d'un dommage collatéral

Au-delà du modèle précis de la *kill chain* qui suppose une véritable organisation pour être mis en œuvre, étant donné les compétences spécifiques pour agir efficacement sur chaque phase de la chaîne, il ne faut en aucun cas écarter l'hypothèse d'un dommage collatéral causé par une cyberattaque de faible niveau. En effet, le modèle d'analyse des cyberattaques du DoD se fonde sur un modèle où les effets sont proportionnels à l'ampleur de la faille, sous-entendant

[7] Agence Nationale de la Sécurité des Systèmes d'Information, « Alerte : multiples vulnérabilités dans des processeurs – comprendre Meltdown et Spectre et leur impact », ssi.gouv.fr, 2018 – https://www.ssi.gouv.fr/actualite/alerte-multiples-vulnerabilites-dans-des-processeurs-comprendre-meltdown-et-spectre-et-leur-impact/.

des investissements en temps et en hommes dans les mêmes proportions. Or, un certain nombre de cyberattaques ont démontré que cette corrélation, si elle est le plus souvent pertinente, n'est pas systématiquement avérée.

L'exemple en 2008-2009 du virus Conficker est à ce titre éclairant. Celui-ci est répandu quelques semaines après que Microsoft ait, dans son bulletin de sécurité mensuel, révélé l'existence d'une faille de sécurité importante (MS08-67) dans ses logiciels Windows 2000, XP, Vista, Seven, Windows Server 2003 et Windows Server 2008. Il s'agit ainsi probablement d'un maliciel créé suite à la révélation de Microsoft, plutôt que de la découverte et l'exploitation d'une faille *zero day*. Toutefois, malgré ce niveau de complexité technique – élaboration d'une arme pour une faille connue – assez faible, Conficker a été un des maliciels les plus dangereux en termes d'extension géographique.

Visant une vulnérabilité dans des systèmes d'exploitation (*operating systems)* particulièrement répandus, il touche en 2009 au total 7 millions d'ordinateurs. En lui-même Conficker n'était pas un maliciel particulièrement dangereux puisqu'il ne détruisait pas les systèmes. Dans ses premières versions, il se contentait de bloquer les mises à jour de sécurité des ordinateurs infectés, à partir de la version C il est en outre capable de se mettre à jour de lui-même pour contrer l'action des anti-virus. Si les auteurs n'ont jamais été identifiés, y compris par absence de revendication, il n'en reste pas moins que Conficker fut l'un des maliciels les plus mystérieux et potentiellement dangereux des années 2000. Il a d'ailleurs infecté des systèmes militaires connectés à Internet – y compris de manière indirecte comme c'est le cas pour les systèmes ISPT (internet sur poste de travail) qui créent *de facto* une passerelle Intradef/Internet – aux États-Unis, au Royaume-Uni et même en France[8].

L'exemple de Conficker montre bien les dangers de la popularité de certains systèmes et logiciels qui ont tendance, justement à cause de leur popularité, à être ciblés par des *hackers*, y compris pour des raisons de compétition entre groupes pirates, pour des effets de réputation le plus souvent.

Toute attaque dirigée contre des systèmes dont la base est un logiciel très populaire (Windows et dérivés, Office, Android, etc.), avec une connexion directe ou indirecte à Internet, risque de toucher les Armées et toute organisation gouvernementale, d'autant plus – Conficker l'a bien montré[9] – que les organisations ont des process de protection beaucoup plus lents à être mis en place.

Cette logique d'une pandémie issue d'un dommage collatéral, par une attaque cyber ne visant pas une désorganisation de la société mais simplement un hacking mettant en lumière une faille sécuritaire, rejoint la vision d'une paralysie par contagion. Elle implique alors une extension progressive de la coupure ou perturbation numérique civile entraînant une paralysie des systèmes gouvernementaux numériques et des capacités de communication, créant un ensemble de difficultés sur les activités économiques et la vie civile générale.

---

[8] Intelligence online, « Comment le virus Conficker a paralysé les armées », intelligenceonline.fr, 5 février 2009 – https://www.intelligenceonline.fr/intelligence-politique/2009/02/05/comment-le-virus-conficker-a-paralyse-les-armees,55783519-eve?.

[9] Sur les 7 millions d'ordinateurs touchés, très peu appartiennent à des particuliers, ces derniers déléguant leur stratégie de mise à jour aux fournisseurs logiciels, contrairement aux organisations qui mettent en place des chaînes de validation, parfois longues, qui laissent plus de temps aux maliciels de se répandre.

1.1.2. La cause non-cyber à effets équivalents

Le modèle de la cyberattaque créant une pandémie numérique repose sur un présupposé : pour créer un effet « pandémique », l'attaque doit obligatoirement viser un logiciel ou un composant qui est particulièrement répandu, présent dans de nombreux équipements aussi bien dans le domaine militaire que civil. Une autre hypothèse mérite ici d'être explorée, le déni d'accès aux équipements numériques par des actions non-cyber, en particulier sur le spectre électromagnétique.

Une attaque – ou une action, même non intentionnellement offensive – sur le spectre électromagnétique, y compris l'hypothèse d'une impulsion électromagnétique (EMP), aurait des effets comparables. En empêchant l'utilisation de composants ou d'appareils électriques, elle créerait un effet similaire à une « pandémie numérique » puisqu'elle aurait mécaniquement un impact à la fois sur les systèmes de traitement de données, aussi bien que sur les réseaux de télécommunications, les deux étant particulièrement sensibles aux effets électromagnétiques.

Plusieurs technologies sont en mesure de créer des effets électromagnétiques plus ou moins importants, qu'il s'agisse des conséquences d'une explosion nucléaire ou d'engins spécifiquement conçus pour créer des perturbations électromagnétiques (*e-bomb*).

Bien qu'il n'existe pas de précédent militaire d'une attaque coupant les communications par action électromagnétique générale, ce type d'agression devient de plus en plus probable dans le contexte d'un hypothétique conflit interétatique. La focalisation des États-Unis sur le domaine de la guerre électronique, au sein des développements technologiques de la *Third Offset Strategy*, résulte en partie de cette crainte, notamment suite au RETEX des opérations russes en Géorgie en 2008[10].

L'hypothèse de l'attaque cyber aussi bien que la perturbation électromagnétique mettent l'accent sur deux vulnérabilités profondes des systèmes cyber militaires : d'une part les bases technologiques qui sont le plus souvent communes avec des appareils civils – sans même parler des technologies duales – et, d'autre part, la question de l'accès aux réseaux de communication.

Cette dernière pose d'ailleurs comme cause non-cyber intentionnelle, le cas d'une attaque contre les moyens physiques de la communication réseau. Il s'agit de créer un chaos général au sein d'un État en coupant le hardware de la communication. L'on pense bien entendu à la destruction des satellites avec un développement toujours plus important des armes destinées à cet effet[11].

Toutefois une telle dimension, caractéristique d'une guerre entre États, n'est pas la seule menace sur les structures physiques. De fait, le cas d'une coupure des câbles sous-marins de télécommunication provoquant avant tout un effet sur les capacités civiles (tout en permettant

[10] Philippe Gros, « La *third offset strategy* américaine », *Défense & Industrie*, n°7, Juin 2016, 3 pages.

[11] Florian Maussion, « Destruction d'un satellite par l'Inde : un acte stratégique aux conséquences imprévisibles », lesechos.fr, 27 mars 2019 – https://www.lesechos.fr/industrie-services/air-defense/destruction-dun-satellite-par-linde-un-acte-strategique-aux-consequences-imprevisibles-1004218.

de garder un anonymat supérieur à la destruction de satellite) est un cas à prendre en compte[12].

Si cette hypothèse n'est pas nouvelle et est prise en compte depuis longtemps par les forces armées, une hausse des activités répréhensibles (cartographie des câbles pour savoir lesquels couper, systèmes d'écoutes en se branchant aux câbles, etc.) tend à désigner ce scénario comme crédible[13].

La cause non-cyber, bien que plus directe et donc davantage couplée à une réponse militaire, constitue une cause directe de conflit. Elle met en exergue un effet général et immédiat sur la société par une paralysie complète des communications sur une zone, voire la totalité d'un territoire (cas d'une rupture massive des câbles). L'impact est alors d'autant plus grand que la totalité de la société, de plus en plus interconnectée, sera privée de communication et d'alimentation réseau, entraînant en plus d'un effet psychologique important une paralysie –plus ou moins durable – du pays.

Dans ce cadre, l'établissement d'un chaos s'avère prévisible du fait des effets cumulatifs d'un arrêt de l'économie, de nombreux accidents, des difficultés de gestion de la crise (pas de communication à distance pour les éléments de secours, arrêt des transports, arrêt de l'alimentation électrique et donc d'une partie des systèmes de soins, arrêt des transactions bancaires, etc.), avec des conséquences majeures qui outrepassent donc les simples effets sur les systèmes électroniques.

1.1.3. L'hypothèse accidentelle ou par cause naturelle

Maintenant que les deux causes intentionnelles de déclenchement d'une pandémie numériques (cyber et non-cyber) ont été évoquées, il s'agit de prendre en considération la question d'une pandémie accidentelle ou naturelle à l'image de la plupart des pandémies sanitaires.

Ce cadre appliqué au cas de la pandémie numérique permet d'envisager deux causes principales, l'accident et la cause naturelle.

Pour ce qui est de l'accident, il s'agit d'une catastrophe civile ayant des répercussions sur les communications mais sans intention de provoquer une paralysie. Par exemple un accident nucléaire civil conduisant à une rupture de l'électricité dans une zone, ou encore une collision de satellites entraînant une perte des réseaux téléphoniques voire de communication. Bien que dans ce cadre l'impact numérique soit limité – soit géographiquement, soit à un vecteur numérique (téléphonie mais pas l'électricité) –, une réelle paralysie d'une partie du territoire est possible.

Le second cas probable constitué par la catastrophe naturelle amène des conséquences bien plus importantes.

---

[12] Laurent Lagneau, « L'OTAN se préoccupe de la sécurité des câbles sous-marins de télécommunications », opex360.com, 24 octobre 2020 – http://www.opex360.com/2020/10/24/lotan-se-preoccupe-de-la-securite-des-cables-sous-marins-de-telecommunications/.

[13] Ibid.

Deux exemples sont particulièrement adaptés au cas d'une pandémie numérique. En premier lieu, une rupture générale de l'approvisionnement électrique d'un pays du fait d'une cause naturelle (comme le tsunami ayant conduit à la catastrophe de Fukushima), et en second lieu, le cas d'une éruption solaire entraînant un blackout général par pannes d'électricité généralisées, satellites hors d'usage, trains et avions paralysés, signalisations hors-service, systèmes GPS brouillés…[14].

Ce second cadre toujours prévisible et anticipé par l'ensemble des gouvernements est pourtant majeur puisqu'aucune parade – hormis l'anticipation – n'est possible. Bien qu'un seul exemple ait eu lieu à l'époque contemporaine, avec en 1989 l'écroulement général du réseau québécois pendant 9 heures, et pour le volet militaire, le contingent australien de la force des Nations-Unies en Namibie qui s'est retrouvé privé de communications, les conséquences seraient dramatiques dans le cas d'un phénomène d'ampleur[15].

Les effets de ces causes naturelles sont directs et surtout durables du fait d'une destruction des moyens physiques de communication et d'alimentation électrique. La paralysie de la société est alors étendue, voire mondiale dans le cas d'une éruption solaire de grande ampleur, entraînant une pénurie de moyens, un chaos généralisé, ainsi qu'une crise civile générale.

L'étude des diverses causes possibles de la pandémie numérique et de leurs effets permet de dresser un bilan du phénomène en termes d'impacts probables sur la société civile.

Ainsi, bien que l'ampleur du phénomène puisse être différente en fonction de la cause de la paralysie, de même qu'elle peut être brutale ou progressive, les conséquences sur la société civile demeurent du même ordre en termes d'intensité ou de points d'application...

Le tableau ci-dessous, en réalisant le bilan de ces conséquences, délivre l'ensemble des champs où le concours de l'armée de Terre pourra être demandé :

Effets de la pandémie numérique	Conséquences sur la société civile
Destruction/paralysie des moyens de télécommunication et de traitement de l'information	*Blackout* partiel ou total entraînant un arrêt ou un frein de l'activité économique, politique et sociale…
Désorganisation des organismes de direction du pays	Difficulté à actionner des moyens de gestion de crise et donc à réguler le chaos ambiant, ainsi qu'à rétablir l'ordre et les communications
Action psychologique	Démoralisation de la population, isolement, panique, mouvements de foules probables
Paralysie des systèmes de transport et des échanges économiques numérisés	Arrêt de l'économie de services ainsi que des capacités d'approvisionnements issues de l'étranger.

[14] Bruno Alvarez, « Faut-il craindre les effets d'une éruption solaire en 2023 ? », ouest-France.fr, 17 juin 2019 – https://www.ouest-france.fr/leditiondusoir/data/52889/reader/reader.html#!preferred/1/package/52889/ pub/76936/page/4.

[15] L'exemple historique le plus frappant est l'éruption solaire de 1859 ayant entraîné la coupure mondiale du télégraphe, exemple qui, s'il était répliqué aujourd'hui, produirait une rupture mondiale des moyens de télécommunication.

Paralysie des capacités de secours	Paralysie des réseaux d'alerte, de communication, d'organisation, et rupture en alimentation des hôpitaux, etc.
Pénuries en besoins vitaux	La rupture des échanges avec l'étranger peut entraîner des pénuries de nourriture. Pénurie en carburant. Pénurie d'alimentation électrique (éclairage, chauffage...).

1.2. La place de l'armée de Terre en cas de pandémie numérique : un usage fortement encadré de l'outil militaire

La définition de la pandémie numérique ainsi que l'étude de sa nature et de ses causes ont permis de définir l'impact probable sur la société civile, avec diverses catégories de perturbations à la résilience de la nation.

Il s'agit désormais de déterminer le cadre probable d'usage de l'armée de Terre en soutien des moyens civils, préalable à l'étude concrète des actions des forces terrestres face à une pandémie numérique.

1.2.1. L'action de l'armée de Terre, un rôle secondaire

Bien qu'elle soit inédite dans sa nature, la pandémie numérique s'inscrit dans la large famille des crises civiles pouvant entraîner un recours aux forces armées pour renforcer la résilience de la nation. La dernière en date, la crise de la Covid, a confirmé une action des armées en soutien face à la crise. En effet, trois grandes catégories d'apports de l'armée de Terre ont été relevées.

En premier lieu, une fonction logistique, organisée en trois volets :

- Transport de matériels : notamment pour les équipements de protection avec la mobilisation des régiments du train pour rapatrier des masques en provenance de Chine vers les entrepôts de Santé Publique France, ou encore celle du 27ème BCA distribuant fin mars des équipements médicaux sur cinquante sites (en majorité des EHPAD)[16].
- Expertise logistique : par deux experts détachés auprès de la cellule de crise de Santé Publique France[17].
- Transport de patients : effectué par hélicoptères caïman (48 patients entre le 18 mars et le 12 avril)[18].

[16] Frédéric Coste, *Contribution des armées françaises à la réponse à l'épidémie de Covid-19*, Fondation pour la recherche stratégique, avril 2020, p. 8.

[17] Ibid. p. 7.

[18] Ministère des Armées, « Opération résilience », defense.gouv.fr, 27 avril 2020 – https://www.defense.gouv.fr/actualites/operations/operation-resilience.

En parallèle de l'action logistique, la principale contribution de l'armée de Terre en termes de volumes a résidé dans une action traditionnelle pour les forces armées sur le territoire national, qu'est la fonction de protection. Ceci s'est traduit en particulier par la protection des hôpitaux et des stocks de moyens sanitaires, suite à un ensemble de vols constatés dans les premiers jours de pénuries[19].

Enfin le dernier volet de l'action de l'armée de Terre dans la participation à la résilience de la nation face à la Covid s'incarne dans une action spécialisée de réponse à la menace. En l'occurrence, il s'agissait en urgence pour les éléments terre du SSA de mettre en place un élément militaire de réanimation (EMR) pour pallier la saturation des capacités civiles[20]. Cet élément déployé en 48 heures ayant permis de créer 30 lits de réanimation.

Plusieurs conclusions transposables au scénario d'une pandémie numérique sont à tirer de l'action de l'armée de Terre dans la lutte contre la Covid.

En premier lieu, dans tous les cas l'action militaire demeure secondaire en ce qu'elle intervient uniquement en renfort des capacités civiles (une logique également présente dans les missions où l'armée prend la plus grande part des opérations[21]), et ne saurait se substituer à leur action qu'en cas d'absence totale de moyens civils. Or, même dans ce cadre elle reste un élément d'appui tandis que la sphère de décision demeure politique et que les moyens privilégiés demeurent civils. Cadre qui serait tout à fait similaire à celui de la pandémie numérique, puisque dans ce schéma les effets impacteront avant tout des moyens civils qui devront être remis en état par des entreprises civiles (électricité, télécommunications, réseaux de transports), auxquelles les forces armées prêteront assistance, restant de ce fait cantonnées à un rôle secondaire puisque la priorité des actions de résilience demeurera du ressort des moyens civils.

Le second enseignement tiré des missions de l'armée de Terre dans la pandémie sanitaire réside dans une définition des grandes catégories d'action dans lesquelles les forces terrestres seront mobilisées pour lutter contre une paralysie des systèmes numériques. Trois volets cumulatifs seront à considérer : une aide logistique ; une action traditionnelle de protection et de maintien de l'ordre ; une aide spécialisée prenant forme dans la mobilisation des régiments directement concernés par le maintien et la création de réseaux numériques (SIC, pôles cyber, régiments fournisseurs d'énergie fossile et électrique).

---

[19] Commission de la défense nationale et des forces armées, « Rapport d'information portant restitution des travaux de la commission de la défense nationale et des forces armées sur l'impact, la gestion et les conséquences de la pandémie Covid-19 », assemblee-nationale.fr, 3 juin 2020 – http://www.assemblee-nationale.fr/dyn/15/rapports/cion_def/l15b3088_rapport-information.

[20] Ministère des Armées, « Opération résilience », op. cit.

[21] Le cas de l'opération sentinelle est ici emblématique. En effet, alors qu'il s'agit d'une opération intégralement militaire entraînant un déploiement massif de forces sur le territoire, celle-ci n'est effectuée qu'en complément des forces de sécurité intérieure pour les aider dans la protection des sites sensibles face au terrorisme. De plus, l'armée ne possède pas dans ce cadre de pouvoirs de police et ne saurait se substituer aux forces de sécurité intérieures : Elise Boz-Acquin, *Le nouveau cadre juridique d'intervention des forces armées en milieu terrestre face au terrorisme*, Fondation pour la Recherche Stratégique, Août 2020, 12 pages.

1.2.2. Une fonction d'assistance consacrée par le droit

L'action de l'armée de Terre en tant que forces de soutien aux moyens civils, et ce quelle que soit l'ampleur de la contribution des armées, si elle est consacrée par les faits (opération *Résilience*), est également régie par le droit qui encadre strictement l'emploi de l'armée sur le territoire national.

Ainsi au titre de la loi, l'armée dans son action de participation à la résilience de la nation est par nature secondaire puisqu'elle est subordonnée à une action de recours. Ce principe de subsidiarité de l'action des forces est incarné dans la règle dite des « 4i » : dans ce cadre, une autorité civile ne peut recourir aux armées que lorsque les moyens civils sont Indisponibles, Inadaptés, Inexistants ou Insuffisants. Principe juridique fruit de la pratique avant d'être institutionnalisé en 2017 par l'« *instruction ministérielle 10100 relative à l'engagement des armées sur le territoire national lorsqu'elles interviennent sur réquisition de l'autorité civile* ».

Ceci implique donc dans tous les cas une action en réaction des forces terrestres, qui devront pallier l'urgence en essayant de combler les lacunes des moyens civils, sans s'y substituer ou en prendre la direction. Le droit organise une fois encore cette dimension hiérarchique en indiquant que le ministre de l'Intérieur est « *responsable de la préparation et de l'exécution des politiques de sécurité intérieure et de sécurité civile qui concourent à la défense et à la sécurité nationale* »[22], tandis que le préfet de zone de défense et de sécurité est pour sa part responsable de la préparation et de l'exécution des mesures de sécurité nationale au sein de sa zone de sécurité.

Par conséquent, dans une crise intérieure, le commandement et la chaîne hiérarchique restent unique et de responsabilité civile : préfet ou ministre. Les forces militaires bien que toujours sous commandement militaires sont subordonnées et agissent en fonction des missions données par l'autorité civile. L'action des forces terrestres face à une pandémie numérique pourra donc uniquement être étudiée dans sa complémentarité aux actions civiles, quand bien même certaines actions seraient conduites en autonomie (patrouilles et maintien de l'ordre) d'autant plus qu'elles seront toujours effectuées sous mandat civil (comme l'opération *Sentinelle*).

À la lumière du rappel de ce cadre juridique contraint, la place occupée par les forces terrestres en cas de pandémie numérique civile restera importante bien que subsidiaire en tant que recours pour porter assistance aux moyens civils.

Dans ce cadre, une comparaison avec l'action lors de la pandémie de la Covid exprime trois fonctions pour lesquelles l'armée de Terre viendra à être mobilisée en cas de pandémie numérique :

- Soutien logistique (stockage, transport) ;
- Missions traditionnelles de surveillance, maintien de l'ordre, et protection ;
- Missions spécifiques à la menace (relais de communication, structures énergétiques d'urgence, structures SIC de secours, etc.).

[22] Article L1142-2 du code de la défense.

Cette première partie désormais achevée aura permis de définir la pandémie numérique, et de mieux la caractériser dans ses effets et impacts probables sur la société civile par une étude de ses causes. Une fois ceux-ci connus, la place attendue pour l'armée de Terre dans son action face à la menace a pu être définie par analogie avec les crises antérieures (en particulier la pandémie de coronavirus) et selon les normes juridiques encadrant l'usage des forces sur le territoire national. Il en ressort une action limitée à une fonction subsidiaire pour un rôle secondaire d'assistance aux moyens civils qui agissent en priorité.

Il s'agit donc à présent d'en caractériser concrètement l'emploi afin de dégager l'apport effectif des forces terrestres à une pandémie numérique pour *in fine* pouvoir en discerner les limites et donc l'impact de la pandémie numérique sur l'action de l'armée de Terre et son propre fonctionnement.

2. Quelles actions pour l'armée de Terre en cas de demande de concours pour faire face à une pandémie numérique ?

Une action concrète des forces terrestres en cas de pandémie numérique impose de mieux cerner les missions qui pourraient être exigées dans la durée à l'armée de Terre. Dans cette optique, en exploitation du rôle définit précédemment, deux domaines complémentaires sont envisageables : une action classique de déploiement sur le territoire pour assurer des missions de logistique, de protection et de maintien de l'ordre ; une action spécialisée pour endiguer la paralysie numérique.

2.1. Des missions générales armée de Terre pour parer aux dysfonctionnements collatéraux engendrés par la pandémie numérique

2.1.1. Cadre de l'action

Ainsi que nous venons de le souligner, les conséquences de la pandémie numérique auraient un effet domino destructeur sur tous les domaines utilisant l'informatique pour le pilotage ou le dépannage.

De ce fait, la vie communautaire et individuelle serait fortement impactée par des dysfonctionnements gênants ou empêchant la distribution des énergies (électricité et gaz) perturbant les transports aériens ou par voie ferré, ou interdisant une partie des transactions bancaires. L'effet conjugué de ces dysfonctionnements conduisant à une sorte de *blackout*.

Ainsi privés de ressources de base, de nombreux citoyens pourraient ressentir un sentiment d'abandon pouvant conduire localement à la panique voire aux émeutes.

Ce constat actuel pourrait en outre s'aggraver à l'horizon de l'étude du fait de l'explosion du nombre d'engins connectés, en particulier grâce à la 5G que ce soit des machines, des appareils domestiques, etc.

Face à une telle situation, les forces terrestres interviennent lorsque les moyens de l'autorité civile sont indisponibles, inadaptés, inexistants ou insuffisants dans un cadre législatif et réglementaire précis sur réquisition du pouvoir ou des autorités civiles en tant que forces de troisième catégorie pour maintenir l'ordre, pour prévenir d'éventuels troubles et rétablir l'ordre Républicain. Ainsi, « *lorsque l'étendue et l'intensité des phénomènes caractérisant une crise ont un impact important sur la vie de la Nation et le fonctionnement de l'État, le Président de la République, peut, en vertu de l'article 15 de la Constitution, décider le déploiement des armées sur le territoire national dans le cadre d'une opération intérieure. Cette décision, arrêtée en conseil de défense et de sécurité nationale (CDSN) permet la rédaction de réquisitions par les préfets de zone de défense et de sécurité*. »[23].

[23] Instruction ministérielle M 10100 du 14 novembre 2017 relative à l'engagement des armées sur le territoire national lorsqu'elles interviennent sur réquisition de l'autorité civile. ABROGEANT L4IM 500 et l'IM du 24 mai 2005.

Le cadre de réquisition lui-même définit donc avant tout un usage des forces terrestres pour des opérations classiques de maintien de l'ordre, à l'image de ce qui a été effectué avec la mise en œuvre de l'opération *Sentinelle*. Il faut par conséquent déterminer l'ampleur de la contribution des forces à une nouvelle opération générale de ce type en cas de crise sanitaire.

En effet, bien qu'un redéploiement des forces de l'opération *Sentinelle* soit envisageable, cela ne peut être la seule solution. Il faudra donc piocher dans les moyens déjà limités des forces terrestres sans empiéter sur les déploiements actuels. Bien qu'en théorie l'armée de Terre puisse disposer de 114 600 militaires[24], les contraintes opérationnelles, administratives, de formation, etc. ont déjà rendu difficile l'armement de l'opération *Sentinelle* qui est allée au bout du contrat opérationnel sur le territoire national en 2015 (10 000 hommes)[25] et surtout entraîne par son maintien dans la durée de nombreuses conséquences négatives sur les forces[26]. La capacité de *surge* dans le cadre d'une pandémie numérique apparaît donc largement contrainte.

Le cadre de l'action ainsi présenté démontre un usage des forces terrestres centré sur le maintien de l'ordre, avec néanmoins des moyens limités.

Toutefois, que ce soit par une augmentation exceptionnelle des effectifs (notamment avec une réquisition des réservistes) ou par une réallocation des ressources dès à présent déployées, l'armée de Terre sera bien présente dans la lutte contre une pandémie numérique pour maintenir l'ordre, assurer des actions logistiques et exercer des missions de protection. Par conséquent, il s'agit à présent d'en détailler les missions probables.

2.1.2. Esquisse des missions

Dans un tel contexte exceptionnel, les missions susceptibles d'être remplies par l'armée de Terre dans l'urgence et en ultime recours, en complément de l'action des services publics ou des unités spécialisées de sécurité civile, consistent à sauvegarder les conditions d'existence des citoyens. Il s'agirait ainsi cumulativement de pouvoir :

- Assurer la protection d'installations d'intérêt général. En particulier celles dont les dispositifs automatisés de surveillance auraient été mis hors d'usage ou qui seraient sujettes au pillage du fait des pénuries provoquées par la pandémie. Ce type de mission ne pose pas de problème du fait des compétences et savoir-faire interarmes détenus par les hommes et femmes de l'armée de Terre.
- Assurer la protection d'itinéraires en particulier pour assurer les missions logistiques et l'acheminement des moyens en situation de pénurie, ainsi que l'évacuation des personnes comme des marchandises.
- Contrôler des zones afin d'endiguer les mouvements de foule ou au contraire d'agir contre l'isolement forcé de certaines zones du fait d'une contestation de l'ordre.

---

[24] Complétées de 4 900 réservistes de la Garde nationale : Ministère des Armées, *Les chiffres clés de la défense : édition 2020* », 2020, pp. 20-22.

[25] Assemblée Nationale, *Rapport d'information sur la présence et l'emploi des forces armées sur le territoire national,* 26 juin 2016, p. 110.

[26] Ibid. pp. 111-117.

- Assurer un ensemble de missions logistiques, en particulier dans le transport de personnels ou de marchandises. Capacité d'autant plus essentielle que la paralysie des transports civils imposera d'utiliser les moyens militaires terrestres pour contrer la pénurie des moyens.

La particularité de ces missions, au demeurant maîtrisées par l'armée de Terre, réside dans des besoins qui ne sont pas concentrés sur une zone donnée comme lors d'inondations ou de tremblements de terre par exemple, mais intéressent un périmètre beaucoup plus important et dans de nombreux domaines de la vie courante. Ainsi, bien que le cadre de l'action soit connu, devant l'ampleur des demandes et du volume des moyens exigés et à déployer sur l'ensemble du territoire, une priorisation des missions sera à mener afin de correspondre au format de l'armée de Terre et de la répartition géographique de ses unités.

Cette vision succincte du cadre des actions classiques de l'armée de Terre sur le territoire national, à savoir celui de la protection, du maintien de l'ordre, et de la logistique, énonce le caractère incontournable des forces terrestres. En effet, bien que les moyens apparaissent comme contraints en termes de volumes, le caractère d'ultime réserve de capacités et d'organisation en cas de crise impose l'armée de Terre comme un acteur central en cas de pandémie numérique. Rôle qui ne pourra qu'être renforcé par le concours de ses moyens spécialisés dans le domaine numérique, dont les missions doivent à présent être étudiées.

2.2. *Les actions spécialisées dans le numérique menées par l'armée de Terre pour parer sur le coup aux dysfonctionnements directs engendrés par la pandémie sur les systèmes et réseaux d'information*

2.2.1. Capacités

À la différence des missions évoquées ci-dessus qui concernent l'ensemble de l'armée de Terre, les missions décrites dans cette partie sont essentiellement du ressort des unités spécialisées dans les communications, la cyberdéfense ou la guerre électronique. Actuellement, une dizaine de régiments de Transmissions font partie de l'ordre de bataille de l'armée de Terre, ils appartiennent soit à la Brigade de transmission et d'appui au Commandement (28e RT, 40e RT, 48e RT, 53e RT et 41e RT), soit à la Brigade de Renseignement (54e RT, 44e RT, ces deux régiments étant spécialisés dans la guerre électronique).

Les régiments de transmission équipés de moyens opératifs et tactiques maintiennent et sécurisent tous les réseaux nécessaires au commandement de la force comme aux interactions des systèmes d'armes. Leurs équipements et les compétences détenues permettent à ces unités de maîtriser l'information de bout en bout, l'information est ainsi acheminée de manière indépendante par rapport aux réseaux commerciaux civils, mais aussi sécurisée, analysée et valorisée dans le cas particulier du SICS[27].

[27] Système d'information et de communication Scorpion.

Rappelons[28] que les SIC sont constitués par :

- Les Systèmes de communication (SC), permettant le transport des flux d'informations à travers des réseaux de télécommunications fixes ou mobiles, déployables en opération.
- Les Systèmes d'Information (SI), assurant le management de l'information et son stockage.
- La Sécurité des systèmes d'information (SSI ou cyber protection) permettant à un système d'information de résister à des évènements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises, et des services que ces systèmes offrent ou qu'ils rendent accessibles.
- Les principaux systèmes permettant d'assurer des liaisons satellitaires (stations ASTRIDE ou HDTAC ou très haut débit SIA box, systèmes RITA…).

Dans le domaine Cyber, l'organisation de la cybersécurité au sein de l'armée de Terre comporte deux volets complémentaires et indissociables, ce sont : la cyberprotection et la lutte informatique défensive (LID) qui est progressivement complétée par la lutte informatique offensive (LIO)[29].

Les moyens ainsi listés présentent une excellente capacité technique avec la possibilité de recréer des réseaux de communication indépendants dans leur entièreté et donc de pallier en soi la principale menace d'une pandémie numérique qu'est un *blackout* général et durable.

En outre, à l'inverse des éléments de forces qui peuvent souffrir d'une nécessité de déploiement non pas localisé mais général (avec la concentration des unités et le transport que cela implique), les régiments spécialisés n'auront pas de mal à se déployer de manière globale du fait d'un excellent maillage territorial des différents régiments de transmission.

La capacité des éléments spécialisés à agir en soutien des moyens civils apparaît donc majeure et efficace, quand bien même elle serait limitée en effectifs à l'image des contraintes déjà évoquées sur les volumes des forces.

Ce premier bilan tiré, il faut à présent entrer dans le détail des actions spécialisées des forces terrestres pour contenir une pandémie numérique, c'est-à-dire faire l'analyse des missions probables.

2.2.2. Esquisse des missions

Les missions spécifiques des forces terrestres, remplies conformément aux règles évoquées dans le chapitre précédent, sont priorisées et déclenchées au niveau national selon les directives émanant des zones de défense, et pourront donc être plus nombreuses en fonction des

[28] Doctrine interarmées DIA-6_SIC-OPS.

[29] Ministère des Armées, « Communiqué – La France se dote d'une doctrine militaire offensive dans le cyberespace et renforce sa politique de lutte informative défensive », defense.gouv.fr, 18 janvier 2019 – https://www.defense.gouv.fr/fre/salle-de-presse/communiques/communique_la-france-se-dote-d-une-doctrine-militaire-offensive-dans-le-cyberespace-et-renforce-sa-politique-de-lutte-informatique-defensive.

régions. De fait, la zone à l'origine de la pandémie nécessitera une intervention plus particulière que les simples zones contaminées (à moins d'un phénomène naturel universel comme les éruptions solaires), de même Paris sera l'objet d'attentions plus particulières du fait d'une nécessité de rétablir au plus vite les moyens de communication des organes politiques et structures critiques de l'État.

Néanmoins, prises dans leur globalité, les missions spécialisées de l'armée de Terre dans la lutte contre une pandémie numérique seront de :

- Renforcer la sécurité des réseaux fixes des infrastructures des zones de défense.
- Déployer et mettre en œuvre des réseaux sécurisés à partir des systèmes opératifs ou tactiques pour suppléer aux dysfonctionnements de certains réseaux civils ou utilisés par l'administration.
- Détacher auprès des administrations ou organismes vitaux des spécialistes et des moyens de cyber défense afin de mieux prévenir les attaques, et d'assurer une diminution du risque de contagion ou une aggravation de la paralysie.
- Contrer la désinformation en désorganisant les centres de propagande, et en assurant la diffusion des messages officiels de l'État auprès de la population dans la mesure du possible.
- Accompagner la manœuvre générale par la neutralisation des capacités de nuisance cyber de nos adversaires.

Dans le cadre de ces missions, celles relevant d'opérations cyber seront menées au niveau interarmées en coordination avec le CALID (Centre d'analyse de lutte informatique défensive) et le CASSI (Centre d'audit de la sécurité des systèmes d'information). Dans ce cadre, outre les moyens de la 807ème compagnie de transmissions qui constitue l'unique unité de cyberdéfense de l'armée de Terre[30], les renforts en spécialistes réservistes du CRPOC (Centre des réserves et de préparation opérationnelle de cyberdéfense) pourraient s'avérer précieux voire déterminants.

Cette partie, désormais achevée, aura permis de livrer une analyse plus fine sur les actions concrètes des forces terrestres dans le cadre d'une pandémie numérique. Le zoom ainsi porté sur les deux champs opérationnels probables que sont la mise en œuvre de missions traditionnelles (maintien de l'ordre, protection, logistique) et spécialisées (SIC, lutte cyber), aura démontré une réelle compétence, fondamentale même pour assurer la résilience de la nation et ce malgré la faiblesse anticipée des moyens en volumes. Les conclusions ainsi tirées étant synthétisées dans le tableau page suivante.

[30] La 807° compagnie est basée à Saint-Jacques de la Lande où se situe également la 785° compagnie de GE.

	Actions classiques de gestion de crise			Actions spécialisées	
Catégories	Rétablissement de l'ordre	Protection	Logistique	SIC	Cyber/guerre électronique
Missions	• Contrôle de zone • Protection d'itinéraires	• Structures critiques • Dépôts de ressources en état de pénurie	• Transport de personnels et marchandises	• Renforcement des réseaux restants • Déploiements de réseaux pour pallier à la neutralisation des moyens civils	• Expertise en soutien des structures civiles • Actions défensives et offensives pour endiguer la contagion et détruire les éléments ennemis
Effets recherchés	Réduction du chaos ambiant et gestion éventuelle des foules.	Maintenir la disponibilité des matériels pour les zones critiques.	Compléter les capacités civiles afin de fluidifier la transmission des moyens sur l'ensemble du territoire (en particulier dans les zones le plus touchées).	Rétablissement des communications critiques pour assurer la continuité des services de l'État.	Participer aux capacités de résilience et à la manœuvre mettant fin aux causes de la pandémie en cas d'origine malveillante.
Limites envisagées	Volume des forces disponibles pour assurer cette fonction sur l'ensemble du territoire.	Volume des forces disponibles pour assurer cette fonction sur l'ensemble du territoire.	Pas les plus importantes même si les capacités de transport ne sont pas illimitées en particulier en cas de véhicules spécialisés (camions-citernes).	Volume de réseaux disponibles, même si le maillage territorial et le nombre de régiments pourraient certainement assurer les communications des structures prioritaires.	Capacités offensives limitées à l'instant T du fait d'une composante des forces nouvellement créées.

3. Quelle résilience propre à l'armée de Terre dans le cadre du scénario « pandémie numérique » ?

Puisqu'ont été décrites la place de l'armée de Terre face à la pandémie numérique et les actions concrètes que cela implique, il s'agit désormais d'étudier le second volet du sujet qu'est l'impact de cette crise, non plus seulement sur la société civile, mais bien sur les forces terrestres elles-mêmes.

Pour ce faire, deux dimensions sont indissociables, en premier lieu l'étude de l'impact sur l'armée de Terre proprement dit, mais également à horizon 2035, l'étude des voies possibles de renforcement des capacités de résilience des forces terrestres. Le tout permettant alors d'en tirer des conséquences pour formuler des recommandations selon la nomenclature DORESE.

3.1. L'impact d'une pandémie numérique sur les forces terrestres : résilience et vulnérabilités

Déterminer l'impact de la pandémie numérique sur l'armée de Terre en tant que telle revient à porter un double regard critique. En effet, l'étude des perturbations envisageables sur le fonctionnement des forces n'est pas suffisante, elle doit être complétée d'une analyse des capacités de résilience de l'armée de Terre qui vont atténuer l'impact de la crise et donc permettre de solutionner certaines problématiques.

Les limites réelles émergeant de ce rapport entre conséquences et capacités de résilience, permettront ainsi de définir les voies à renforcer à horizon 2035.

3.1.1. Étude des conséquences probables sur les capacités de l'armée de Terre

L'impact de la menace sur l'armée de Terre face aux scénarios de la pandémie numérique s'avère particulier du fait de sa nouveauté et de sa spécificité. En effet, la menace numérique en tant que telle n'est pas nouvelle et a déjà été soigneusement prise en compte au sein des armées dans les concepts de guerre de l'information[31] ou de guerre électronique[32].

Cependant, même au niveau militaire *stricto sensu* avec l'utilisation contemporaine de moyens civils puissants dévoyés de leur utilisation normale et de spécialistes œuvrant dans la clandestinité, la donne change et l'info valorisation d'une force moderne peut se trouver contestée par des États ou des organisations hostiles. Par ailleurs, les cibles des actions de la fin du XX° siècle visaient essentiellement les centres de commandement qui concentraient les moyens numérisés alors qu'aujourd'hui la généralisation des systèmes numérisés jusqu'au niveau du combattant individuel permet de générer des effets désorganisateurs voire destructeurs à tous les niveaux. L'impact d'une pandémie numérique sur le fonctionnement des forces outrepasse donc la simple gestion par les moyens de guerre électronique.

[31] *Information Warfare.*

[32] *Electronic Warfare.*

Trois domaines de l'armée de Terre seraient ainsi directement impactés :

- **Les capacités opérationnelles de réaction face à la crise** :

Ce type de paralysie profonde des systèmes numériques aurait ainsi bien entendu des répercussions majeures en tout premier lieu sur le domaine des SIC. Les opérations militaires contemporaines sont devenues depuis une vingtaine d'années de plus en plus dépendantes des communications, que ce soit de manière positive (interarmisation des opérations, lien avec les alliés, réactivité des forces, etc.) ou même de manière négative (impact du facteur image sur les forces armées, influence adverse, etc.). Dans une situation qui priverait soudain les forces d'un accès sans cesse plus important aux communications, l'impact sur les opérations serait majeur dans les dimensions de la coordination (interalliée et interarmées) comme de l'action.

Alors que l'essentiel du travail sur la numérisation des communications – et plus largement de l'espace de bataille – a porté sur le raccourcissement de la boucle OODA, notamment par une abolition des distances entre décideurs et acteurs permise par le numérique, celle-ci tendrait ainsi mécaniquement à se rallonger, modifiant *de facto* le tempo des opérations d'assistance aux moyens civils. En conséquence, cette situation risque d'isoler de manière plus marquée les unités subordonnées et obligerait à confier une autonomie plus grande aux échelons de commandement subalternes.

De manière collatérale, les systèmes de renseignement techniques seraient tout autant touchés, notamment en empêchant le prétraitement numérique des différentes productions (image, électromagnétique, etc.) ainsi que leur fusion. L'impossibilité de faire appel à certains capteurs extrêmement dépendants des flux de communication numériques, comme les drones ou la localisation GPS et l'identification amis-ennemis, risquerait fortement d'obérer les capacités de connaissance de l'environnement pour les forces.

Au-delà, une telle paralysie contraindrait également les forces terrestres de nouvelle génération – format Scorpion – à fonctionner en mode « dégradé » avec l'incapacité de bénéficier de la couche numérique de fusion des données des combattants, pourtant au cœur de la numérisation des forces terrestres. L'armée de Terre serait ainsi contrainte de fonctionner avec un niveau technologique équivalent à celui des années 1990, en se fondant ici sur une résilience obtenue par le recours à une « dégradation technologique » (ex : systèmes de communication analogiques, transmission des documents sous forme écrite, etc.).

Enfin, il importe de considérer qu'outre les fonctions citées ci-dessus, l'ensemble des fonctions opérationnelles et de soutien de l'armée de Terre serait touché. En termes de MCO, une absence d'accès aux différents documents de planification des cycles de maintenance créerait ainsi une friction dans l'entretien, provoquant potentiellement des ruptures de capacité à terme, si la pandémie venait à durer. Identiquement par manque d'accès aux dossiers médicaux des personnels militaires, il serait plus complexe pour le SSA de prendre en compte les blessés en opérations ainsi que les victimes éventuelles durant le maintien de l'ordre et les actions sur le territoire national sans risques ou contrindications.

- **Les systèmes terrestres** :

Au-delà des capacités opérationnelles qui seraient forcées à agir en mode dégradé et auraient sur le long terme des difficultés logistiques, il faut prendre en compte également la possibilité de la paralysie complète de systèmes et donc l'impossibilité pour l'armée de Terre de recourir à ses moyens spécialisés, que ce soient des véhicules ou des capacités numériques et énergétiques. Bien que relevant des forces navales, l'exemple des Rafales cloués au sol en 2009 par le virus informatique *Conkficker*, ayant circulé au travers du service informatique du ministère des Armées jusqu'à la structure de vol de la Marine, est particulièrement révélateur[33] (il avait également infecté le 8ème régiment de Transmissions). Une paralysie des capacités terrestres spécialisées (SIC) ou même de moyens logistiques par une impossibilité de traiter les besoins, commandes, ordres de déplacement, etc. entraînerait à la fois une paralysie des systèmes capacitaires et des opérations, diminuant d'autant la capacité des forces terrestres à participer à la résilience de la nation.

- **L'organisation et le commandement ministériel** :

Au-delà des capacités terrestres en tant que telles, une paralysie des canaux de communication et donc de diffusion des ordres, entièrement numérisés ou par le biais des télécommunications, entraînerait un isolement de fait de la plus haute hiérarchie militaire vis-à-vis des régiments. Une conduite globale et coordonnée des moyens terrestres sur l'ensemble du territoire deviendrait donc impossible, du moins à court terme. Dans ce cadre, une décentralisation totale du commandement doit être envisagée avec une mobilisation des forces au cas par cas et en autonomie en fonction de la réquisition civile locale des forces. Bien que réponse en théorie optimale, la pratique serait plus complexe. De fait, un chaos national issu d'une pandémie numérique comme toute crise majeure implique une action planifiée et coordonnée pour produire des effets et éviter une plus grande désorganisation (opérations *Sentinelle, Résilience*…), rôle dévolu traditionnellement aux armées comme ultime garantie en cas d'effondrement des moyens civils. Or l'impossibilité de communication et de transmission directe des ordres rendra très difficile une action organisée, globale et planifiée nationalement, fragilisant la capacité de l'armée de Terre à réellement endiguer les effets directs et indirects de la pandémie numérique (du maintien de l'ordre jusqu'au déploiement de moyens spécialisés). De même au niveau local, l'impossibilité d'user de moyens de télécommunication rendrait partielle et délicate la mobilisation des personnels et systèmes non présents au régiment (retour de vacances, retour des personnels en formation ou en stages régimentaires, etc.) ainsi que la transmission des ordres et leur adaptation au jour le jour.

En résumé, l'ensemble des fonctions et capacités de l'armée de Terre serait impacté directement ou indirectement par une pandémie numérique. Les principales conséquences étant un ralentissement majeur des différentes capacités opérationnelles et de déploiement sur le territoire national, ainsi que des cycles logistiques et de maintenance, handicapant les forces (voire devant compter avec des systèmes intégralement paralysés) et les obligeant à modifier les rythmes opérationnels, et enfin une limitation très importante de la planification et de la transmission des ordres à tous les niveaux. Si rien ne s'opposerait, *a priori*, à la mise en œuvre

[33] Olivier de Robillart, « Le virus Conficker touche la Marine française et ses Rafales », silicon.fr, 9 février 2009 – https://www.silicon.fr/le-virus-conficker-touche-la-marine-francaise-et-ses-rafales-33931.html.

et au maintien des opérations, leur efficience serait néanmoins très fortement dégradée, avec un recentrage sur l'échelon local et la disponibilité des appuis et soutiens au plus près.

3.1.2. Des capacités de résilience de l'armée de Terre face à une pandémie numérique civile

Maintenant que les conséquences probables sur les forces terrestres sont connues, il importe de leur opposer les capacités de résilience qui seront mises en œuvre par l'armée de Terre afin de les minimiser et donc d'en atténuer l'impact réel sur une aide aux moyens civils.

A. Le mode dégradé, une solution de court terme

La parade traditionnelle et unique, issue de la guerre électronique, en cas de milieux électromagnétiques contestés réside dans la mise en œuvre des moyens dégradés[34]. C'est-à-dire de manière succincte l'abandon des capacités numériques (GPS, communication par satellites…) pour garantir la continuité de l'action avec les capacités humaines et mécaniques. Dans ce cadre, la résilience face à une pandémie numérique s'exprime à travers de nombreuses possibilités, avec notamment un retour aux ordres écrits et à une navigation et planification usant de la carte et de la boussole. En outre, un ensemble de capacités palliatives peuvent être envisagées, comme par exemple en matière de télécommunications un déploiement massif de radios à ondes courtes permettant au moins au plan local de retrouver un ensemble de communication déporté direct[35].

Le passage en mode dégradé n'impliquerait donc pas un abandon des capacités et présente une certaine capacité d'adaptation. Toutefois, dans le cadre d'une pandémie numérique, cette solution ne peut s'envisager que pour le court terme sous peine de rendre très limité l'apport des forces terrestres à la résilience de la nation.

En effet, il paraît impossible de fonctionner pendant plusieurs mois sans systèmes spécialisés puisque l'apport premier face à une pandémie numérique sera dans la mise à disposition des structures SIC, or l'aide d'urgence demandée à l'armée de Terre ne pourrait se faire dans ce cadre si un usage de l'action en dégradé est généralisé.

De même, le volet logistique implique une structure de communication et de numérisation afin de permettre une planification de long terme et une organisation des convois de matériels et le transport des soldats et civils en cas de besoins d'évacuation.

La solution de résilience par usage de moyens dégradés, bien que nécessaire dans un premier temps puisque seule à même de limiter les effets de la pandémie numérique sur les forces terrestres, ne peut constituer une solution de long terme. En effet, ceci reviendrait à ne pouvoir être réellement efficace que sur le volet des dimensions non techniques comme le maintien de l'ordre et la protection, et encore de manière localisée. D'autres solutions devront par conséquent être envisagées et anticipées à horizon 2035 pour assurer la résilience de l'armée de Terre.

---

[34] Ministère des Armées, *Stratégie Spatiale de Défense,* 2019, p. 43.

[35] Paul Wohrer, Bruno Lassalle, Jonathan Jay Mourtont, Celia Cornec, *Évolution du contexte spatial : Quelle ambition pour l'armée de Terre ?*, Fondation pour la Recherche Stratégique, Observatoire armée de Terre 2035 : étude annuelle n°2, 2019, pp. 25-27.

B. *L'apport de l'armée de Terre face à une pandémie numérique : des moyens limités*

Après l'impact sur les forces en tant que telles, et les moyens propres de résilience face aux effets directs de la pandémie numérique (moyens dégradés), il convient d'analyser les capacités de résilience indirectes c'est-à-dire celles concernant la capacité à réaliser les missions d'assistance aux moyens civils dans la durée.

En effet, bien que limite principale à la résilience des forces terrestres, le mode dégradé utilisé à long terme n'est pas la seule faille.

Ainsi, même en cas d'une possibilité d'assurer des missions auprès de la population et d'assistance aux moyens civils notamment dans le cadre des aides logistiques et des missions classiques de maintien de l'ordre et de protection des sites sensibles, les moyens dédiés seront limités. Nous retrouvons ici une crainte déjà exprimée dans l'étude des missions concrètes de l'armée de Terre, qu'il appartient à présent de détailler.

En premier lieu, en ce qui concerne les moyens spécialisés directement mobilisés pour rétablir les communications critiques, la fonction SIC *stricto sensu* au sein des forces terrestres ne comprend que 5 régiments, pour 4 900 personnels (en 2016) y compris ceux des fonctions administratives et du Commandement SIC des forces[36].

En outre, les réservistes spécialisés immédiatement disponibles, issus de la réserve citoyenne cyber, sont de l'ordre de 400 avec une possibilité d'en déployer par la suite 4 000 mais avec une formation complémentaire et sur la base du volontariat[37], offrant donc un complément de force peu volumineux.

Les moyens sont donc limités pour faire face à une crise nationale, d'autant qu'une mobilisation de l'ensemble de ces capacités n'est pas possible puisqu'une partie d'entre elles sera d'ores et déjà déployée à l'instant T sur les théâtres extérieurs.

Une problématique d'ailleurs commune en second lieu à l'ensemble des capacités terrestres, qui ne disposent pas d'effectifs pléthoriques et doivent bien entendu en mobiliser une large partie pour les opérations extérieures et missions de souveraineté. Ainsi en octobre 2020, environ 30 000 personnels des forces armées sont mobilisés pour couvrir l'ensemble des missions des armées, avec plus de la moitié supportée par les forces terrestres[38].

---

[36] Ministère des Armées, « Armée de Terre, organismes et formations rattachées : SIC », defense.gouv.fr, 1er juillet 2020 – https://www.defense.gouv.fr/terre/l-armee-de-terre/le-niveau-divisionnaire/commandement-sic-des-forces/commandement-sic-des-forces/organismes-et-formations-rattaches.

[37] Ministère des Armées, *La réserve de cyberdéfense : guide explicatif*, 2020, pp. 8-11.

[38] Frédéric Coste, *Contribution des armées françaises à la réponse à l'épidémie de Covid-19*, op. cit.

Source : Ministère des Armées, 15 octobre 2020 – https://www.defense.gouv.fr/operations/rubriques_complementaires/carte-des-operations-et-missions-militaires.

L'on envisage mieux à la lumière de ces rappels, la possibilité limitée pour les forces terrestres de délivrer une assistance globale à la résilience de la nation. Les actions devront être ciblées et nécessairement circonscrites afin d'être en cohérence avec les effectifs et capacités spécialisées disponibles à l'instant T. Logique qui renforce le cadre secondaire du rôle de l'armée de Terre dans la lutte contre une pandémie numérique civile, qui au-delà de son encadrement juridique et de ses missions pratiques cantonnées à l'assistance, doit composer avec des moyens limités[39].

L'impact de la pandémie numérique sur les forces, de même que l'étude des limites afférentes aux capacités de résilience de l'armée de Terre permettent de discerner un ensemble de faiblesses actuelles face à ce type de crise. Ainsi, dans une vision prospective, il convient désormais d'étudier à horizon 2035 les voies possibles de renforcement de la résilience des forces terrestres.

3.2. Développer les capacités de résilience numérique à horizon 2035

Avant de formuler de possibles solutions pour l'armée de Terre concernant le renforcement de ces capacités de résilience, il semble opportun de réaliser un tour d'horizon succinct des initiatives des autres puissances en la matière, afin de servir d'inspirations pour les forces françaises permettant par la suite d'en dégager des recommandations exprimées sous format DORESE.

[39] Ibid.

3.2.1. Comment les grandes puissances envisagent-elles un renforcement de leur résilience numérique ?

L'hypothèse d'une attaque cyber ou de perturbation des communications touchant directement les forces est une menace prise en compte depuis le début de la numérisation des forces, avec un pic au début des années 2000 en réaction aux attaques russes contre les organes gouvernementaux de l'Estonie (2007) et durant la guerre de Géorgie (2008)[40]. C'est d'ailleurs à la suite de celles-ci que le centre d'excellence de l'OTAN en cybersécurité a été mis en place à Riga (Estonie), et qu'une stratégie en matière de défense cyber a été produite, régulièrement réaffirmée depuis[41].

Toutefois, l'hypothèse d'une pandémie numérique civile touchant également les forces armées et paralysant l'ensemble des communications est un défi nouveau qui émerge à peine dans la réflexion stratégique des grandes puissances. Ainsi à l'heure actuelle, seuls les États-Unis ont évoqué officiellement la conduite d'expertises et études sur une transposition de la pandémie de la Covid à un scénario numérique[42]. Cette prise de conscience assez tardive n'en est pas pour autant anodine et énonce l'intérêt grandissant des autres puissances dans une préparation à une crise numérique, et par conséquent à un renforcement des capacités de résilience.

Si l'on se concentre sur celles-ci, l'on constate deux types de mesures possibles en fonction de leur temporalité.

Ainsi, en premier lieu, des mesures de court terme sont envisagées afin de renforcer les structures critiques et la redondance de moyens afin de diminuer la pression sur les moyens terrestres. Deux exemples sont alors particulièrement révélateurs. Dès 2013 et les fuites de données de l'affaire Snowden, un retour des transmissions de données critiques et de renseignement au format papier par la réintroduction des machines à écrire a été constaté en Europe, en particulier en Allemagne[43]. La Russie a emboité le pas à cette initiative, en la complétant même en 2014 d'une remise en service des échanges interministériels par tubes à Moscou afin d'éviter tout piratage ou coupure électromagnétique[44]. Ces initiatives renforçant les capacités dégradées – dès l'avant crise – sont complétées par une redondance des serveurs et systèmes de communication cyber en particulier au sein des organes ministériels. Cette transformation numérique passe autant par une mise à niveau du *software* (procédures de sécu-

[40] Laurent Lagneau, « La Russie attaque la Géorgie dans le cyberespace », opex360.com, 11 août 2008 – http://www.opex360.com/2008/08/11/la-russie-attaque-la-georgie-dans-le-cyberespace/.

[41] OTAN, « Cyberdéfense », nato.int, 20 octobre 2020 – https://www.nato.int/cps/fr/natohq/topics_78170.htm.

[42] Morgan Dwyer, « Prioritizing weapon system cybersecurity in a post-pandemic defense department », Center for strategic and international studies, csis.org, 13 mai 2020 – https://www.csis.org/analysis/prioritizing-weapon-system-cybersecurity-post-pandemic-defense-department.

[43] Roland Gauron, « Espionnage : l'Allemagne envisage le retour de la machine à écrire », lefigaro.fr, 16 juillet 2013 – https://www.lefigaro.fr/international/2014/07/16/01003-20140716ARTFIG00193-espionnage-l-allemagne-envisage-le-retour-a-la-machine-a-ecrire.php.

[44] AFP, « Russie : la machine à écrire réintègre les services secrets », lexpress.fr, 12 juillet 2014 – https://www.lexpress.fr/actualite/monde/europe/russie-la-machine-a-ecrire-reintegre-les-services-secrets_1265864.html.

rité, serveurs, récupération des données) que d'une modernisation du *hardware* en remplaçant les systèmes informatiques[45]. En outre, a été étudiée une augmentation de la participation des réserves au maintien de l'ordre et à l'aide spécialisée dans un rétablissement des moyens cybers. L'objectif étant de dégager une augmentation des volumes des forces en urgence, avec comme cas le plus emblématique aux États-Unis la réquisition obligatoire et à durée indéterminée de tous les membres de la Garde Nationale[46].

À plus long terme, l'étude des initiatives des autres États démontre une stratégie capacitaire orientée à part entière sur le renforcement des capacités de résilience face à une contestation massive des moyens électromagnétiques.

En termes de capacités militaires *stricto sensu*, il s'agit d'une planification indépendante d'une mise à niveau et augmentation du volume des moyens SIC sur le long terme. Dans ce cadre, le Royaume-Uni est particulièrement novateur, avec la mise en place d'un nouveau programme d'armement devant initier une remontée en puissance capacitaire des SIC jusqu'en 2040[47].

Toutefois, l'innovation la plus importante en matière de lutte contre une pandémie numérique est celle formulée par les États-Unis qui nomme directement cette éventualité. Ainsi un ensemble d'analyses du DOD suite au Covid sur l'ensemble des menaces invisibles pouvant avoir un impact global et entraîner une réponse majeure de la part des forces armées a mis en avant une émergence de la question d'une pandémie numérique dans le débat stratégique, avec comme conclusion que cette menace deviendra à moyen terme un point d'intérêt doctrinal fondamental[48].

Trois conséquences pratiques ont été tirées de ces études dans le cadre de la *Cyberespace Solarium Commission*[49] :

- En premier lieu, il a été établi la production annuelle d'un rapport sur les vulnérabilités cyber des systèmes en dotation dans les forces armées, afin de les combler et d'anticiper l'apparition de nouvelles fragilités.
- En second lieu, il a été fait état de la vulnérabilité de l'ensemble des systèmes électroniques et numériques qui n'ont pas été développés d'entrée dans une logique de défense cyber, par une possibilité d'intrusion dans les systèmes par le biais des porteurs dérivés comme les radios, radars, etc.

  De ce fait l'une des principales recommandations de la commission, pour réduire la vulnérabilité des armées et augmenter leur résilience, est d'insérer dans l'ensemble

[45] Logique ayant même fait l'objet en Allemagne d'une programmation capacitaire insérée dans la stratégie de numérisation et infovalorisation des forces armées, entraînant la production d'un document stratégique mis à jour annuellement : Bundesministerium der Veiteidigung, *Premier rapport sur la transformation numérique du ministère fédéral de la défense*, Berlin, Octobre 2019.

[46] Nicole Vilboux, *Le department of defense américain face à la pandémie de Covid-19,* Fondation pour la Recherche Stratégique, 15 mai 2020.

[47] Army headquarters, *Delivery of tactical communications in the 21th century: an exploration of the Land environment tactical CIS and MORPHEUS programmes*, Royal signals institution, septembre 2019.

[48] US cyber command, « During global pandemic, USCYBERCOM trains virtually to defend networks, protect nation », cybercom.mil, 22 juin 2020 – https://www.cybercom.mil/Media/News/Article/2227651/during-global-pandemic-uscybercom-trains-virtually-to-defend-networks-protect-n/.

[49] Morgan Dwyer, « Prioritizing weapon system cybersecurity in a post-pandemic defense department », op. cit.

des programmes capacitaires futurs une dimension de défense cyber et d'un fonctionnement garanti en milieu électromagnétique contesté ou à tout le moins que la paralysie du système n'entraîne pas une défaillance d'autres systèmes par contagion[50].

- Enfin, afin de garantir une véritable réactivité de la capacité de défense cyber globale aux États-Unis en particulier face à un scénario de pandémie civile globale, ont été définis et réalisés de nouveaux exercices (avec création d'une nouvelle plateforme de simulation) d'assistance à une catastrophe numérique civile ou face à des attaques sur les organes gouvernementaux[51].

3.2.2. Développer les capacités de résilience numérique de l'armée de Terre

Bien que les exemples des programmes et initiatives de pays étrangers répondent avant tout aux spécificités de chaque État, ils peuvent servir d'inspirations pour l'armée de Terre en dégageant des pistes de réflexion pertinentes dans l'appréciation de la menace et les voies envisagées pour la solutionner.

Ainsi, en prenant en compte ce cadre d'inspiration – et surtout – les limites précédemment évoquées des forces terrestres dans une aide à la résilience de la nation dans le cadre d'une pandémie numérique, un ensemble de leçons peut être formulé *a priori*.

En premier lieu, le tour d'horizon des initiatives étrangères de renforcement des capacités de résilience numérique aura démontré une logique double entre mesures de courts termes, et planifications de long terme. L'intérêt étant de prendre en compte qu'une logique de renforcement de ces capacités ne peut être immédiate, et que comme toute dynamique capacitaire elle doit s'inscrire dans une logique de remontée en puissance sur le long terme du fait tant de contraintes budgétaires que d'une évolution progressive des technologies qu'il faudra anticiper et incrémenter au fur et à mesure. Par conséquent, si un ensemble de palliatifs de court terme peut être envisagé pour diminuer la pression sur les forces, ce n'est qu'à long terme qu'est envisageable une réelle mise à niveau des capacités de réaction face à une pandémie numérique.

En outre, la faiblesse des moyens spécifiques à la résilience électromagnétique et cyber, de même que la dépendance des forces aux structures civiles en la matière (en particulier au niveau ministériel et régimentaire) imposent une plus grande intégration des capacités civiles et militaires dès l'avant crise. L'enjeu étant de développer des moyens dégradés communs, ainsi qu'un process de déploiement et d'actions en cas de pandémie numérique par la conduite régulière d'exercices et de simulations.

Enfin, le problème fondamental de l'action de l'armée de Terre étant son manque de volume (en termes de personnels disponibles) pour assurer une action élargie sur l'ensemble du ter-

[50] L'infovalorisation ayant pour ambition de lier tous les systèmes d'une zone d'opération, donc potentiellement aussi de tous les infecter s'il n'y a pas des mécanismes d'isolation en cas d'une attaque cyber, d'une action dans une zone électromagnétique contestée globale, ou d'une pandémie numérique civile.

[51] US cyber command, « During global pandemic, USCYBERCOM trains virtually to defend networks, protect nation », op. cit.

ritoire, une réflexion approfondie doit être menée sur la mobilisation des réserves (spécialisées ou non) tant pour pallier l'urgence que pour, par la suite, maintenir une capacité dans la durée.

En exploitation de ces grandes leçons déduites de cette note de recherche, ainsi que d'une volonté de répondre aux autres problématiques de l'apport de l'armée de Terre à une pandémie numérique civile, un ensemble de recommandations a été produit sous format DORESE et intégrant des initiatives pour le court et le long terme.

Pistes de réflexion à retrouver dans le tableau ci-dessous :

	Court Terme (2025)	Long Terme (2035)
Doctrine	➡ Insérer dans les scénarios de crises nationales le cas de la pandémie numérique pour développer au plus tôt une doctrine et un ensemble de procédures civiles et militaires. ➡ Définir un nouveau cadre d'emploi de la réserve afin de lui donner une dimension opérationnelle plus affirmée et de déploiement d'urgence massif en cas de crise interne (notamment par la rédaction d'une doctrine d'emploi de la réserve cyber).	➡ Mettre en place un organe national d'étude et de simulation des catastrophes cyber permettant par la conduite d'exercices réguliers d'établir annuellement la liste des failles à corriger. ➡ Envisager la mise en œuvre éventuelle d'une réelle dissuasion cyber : une des parades à la pandémie numérique étant un renforcement des moyens cybers, il faut aussi bien envisager les capacités défensives qu'offensives afin de créer une capacité suffisamment efficace pour créer chez l'adversaire une crainte des représailles permettant de réduire en partie les causes intentionnelles de création d'une pandémie numérique cyber.
Organisation	➡ Anticiper le rôle attendu des forces terrestres par zone de défense militaire en fonction des divers scénarios de la pandémie numérique. L'enjeu étant de définir une liste des unités et fonctions mobilisables et de leurs missions dès le temps de paix, pour une activation dès les premiers signes de crise numérique (une sorte de 'plan blanc du numérique'). ➡ Réorganiser les anciennes compagnies de réserve des régiments de transmission afin de les orienter vers une action de défense cyber et numérique en complément de la réserve spécialisée interarmées cyber. ➡ Renforcer le rôle des zones de défense afin que, compte tenu du caractère centralisé de la nation, l'on puisse diminuer l'impact sur les systèmes centralisés en développant la capacité d'action locale et autonome.	➡ Insérer au sein des structures SIC de chaque régiment spécialisé un organe dédié à la formation des personnels aux cas de pandémie numérique civile permettant à terme de définir un process en cas de crise. ➡ Transformer les compagnies spécialisées des régiments SIC en unités de zone de défense spécialisées pour la lutte contre la pandémie numérique (avec une logique interarmées et civilo-militaire). ➡ Créer une unité de protection civile spécialisée dans le rétablissement des communications.
Ressources humaines	➡ Accélérer le recrutement de la réserve citoyenne spécialisée et permettre sa réquisition obligatoire à durée indéterminée (non plus comme actuellement sur la base du volontariat pour les réservistes non opérationnels) afin d'augmenter la masse critique en spécialistes du numérique.	➡ Renforcer les régiments spécialisés par un recrutement ciblé en personnels qualifiés en moyens SIC, et informatiques. ➡ Développer les formations régimentaires de réaction aux crises civiles numériques.

Équipements	➡ Durcissement des SC et SIC contre les menaces électromagnétiques et issues du monde civil. ➡ Préserver les anciennes capacités spécialisées afin d'équiper sans surcoût les nouvelles forces de réserve dans l'optique d'un maillage du territoire. ➡ Acquisition de moyens dégradés pour les structures de communication critiques (machines à écrire, radios à ondes courtes, etc.). ➡ Massification des moyens de relais et communications militaires pour développer le maillage territorial en cas de pandémie numérique nationale. ➡ Réaliser un audit tous les cinq ans des systèmes spécialisés utilisés par la sécurité civile pour juger de leur réelle protection par rapport aux risques cyber et développer des correctifs au plus tôt.	➡ Privilégier l'ascendant du militaire sur le civil dans la conception des futurs systèmes d'armes. ➡ Insérer dans le développement de l'ensemble des programmes capacitaires une dimension de protection cyber et contre les perturbations électromagnétiques afin de diminuer les risques à la source. ➡ Veiller à la mise à la hauteur des systèmes de communication militaires en imposant aux constructeurs une indépendance technique avec les systèmes civils pour réduire le risque de contagion.
Soutiens	➡ La logistique ayant un rôle majeur dans l'apport aux moyens civils dans le cadre d'une pandémie numérique, une logique générale de renforcement de ses capacités de projection, de transports et de ses capacités à durer (MCO améliorée) est à envisager. Elle ne pourra toutefois qu'être continue d'où son insertion à parts égales sur les deux trames temporelles.	
Entraînement	➡ Développer les savoir-faire techniques à tous les niveaux. ➡ Simulation annuelle d'une pandémie numérique mobilisant les acteurs civils et militaires concernés afin de dégager les failles à combler et établir au fil du temps un process d'action. ➡ Mise en place d'exercices de tous niveaux (de la compagnie à la division) d'actions de soutien et de maintien de l'ordre en mode dégradé. Une dimension interalliée de ces exercices est à envisager afin de renforcer l'interopérabilité et la gestion commune de crise en cas de pandémie numérique internationale. ➡ Mise en place de simulations de niveau État-major d'une planification et transmission d'ordre nationale aux régiments en mode dégradé. ➡ Enseigner les réflexes de passage en mode dégradé qui privilégient une dégradation partielle au juste niveau à un arrêt d'emblée systématique.	➡ Création d'une entité militaire de simulation de catastrophes cyber (à l'image du CENTAC) testant les unités sur l'action en mode dégradé aussi bien pour des opérations extérieures que sur le territoire national. ➡ Mise en œuvre d'une certification TTA des unités pour l'action en mode dégradé avec des drills réguliers en régiment (à l'image des entrainements NRBC).

Conclusion

La présente étude avait pour objectif l'analyse des effets d'une pandémie affectant le numérique, à savoir l'interruption brutale et durable des moyens de communication et de diffusion et de traitement de l'information, voire dans sa forme la plus grave, une coupure des alimentions énergétiques électriques et gazières.

Bien que les origines, les causes et les conséquences de la pandémie numérique soient diverses, entre actions intentionnelles, accidentelles voire naturelles, et localisées ou généralisées, une synthèse de ses effets peut être établie. Dans tous les cas, l'on constate une rupture des moyens de communication et d'alimentation électrique, ainsi qu'une paralysie des transports, un isolement des populations, et des pénuries de moyens pouvant entraîner des troubles à l'ordre public.

Dans ce cadre, l'armée de Terre mobilisée en tant qu'ultime recours et organe exceptionnel de gestion de crise a un rôle primordial à jouer. Toutefois, son emploi sera limité à une place subsidiaire, du fait d'un cadre légal définissant précisément le recours aux moyens militaires sur le territoire, que pour les actions envisagées dont l'objectif sera de palier les défaillances des organes civils (règle des 4i).

Les missions envisagées dans cette optique, comme dans toute opération de gestion de crise sur le territoire national, sont de deux ordres :

- **Spécifiques aux forces terrestres** : protection de zones sensibles, logistique, rétablissement de l'ordre.
- **Spécialisées à la crise** : en l'occurrence dans un rétablissement des capacités numériques, une lutte contre la menace, et une assistance aux organes de l'État avec les unités spécialisées.

Au-delà de la définition de la menace qu'est la pandémie numérique, et du rôle concret des forces terrestres pour l'endiguer sur le territoire national, ce travail de recherche a également conduit à déterminer l'impact de ladite pandémie sur l'armée de Terre.

Il en ressort une certaine capacité à agir malgré la crise, avec notamment le recours à une action en mode dégradé et décentralisée permettant de maintenir les communications opérationnelles.

Cette capacité pourrait toutefois être notablement limitée pour deux raisons majeures :

- **Le mode dégradé ne peut s'inscrire dans la durée** : sans quoi il implique une perte de compétences, et donc d'efficience, trop grande en particulier pour les actions spécialisées.
- **Les moyens en dotation sont limités** : le volume des forces disponibles étant relativement faible du fait du format actuel et des contraintes opérationnelles déjà en cours et d'une capacité de recours aux réserves actuellement insuffisante.

Face à ce constat, une analyse des voies de renforcement des capacités de résilience de l'armée de Terre face à une pandémie numérique a été conduite, en s'intéressant aux initiatives étrangères en la matière. Des leçons ont pu en être tirées (nécessité d'agir sur le long terme, obligation de renforcer l'intégration des moyens civils et militaires spécialisés, problème critique des volumes de personnels disponibles), qui ont permis la réalisation de recommandations à court et long termes au format DORESE.

De toutes ces propositions une priorité émerge : l'organisation et le rôle des réserves dans le futur.

En effet, l'étude de la pandémie numérique a permis de mesurer la capacité des forces à intervenir et exercer des effets dans une situation de crises multiples. Cette capacité bien réelle qui peut s'organiser en tirant le meilleur parti de l'organisation des zones de défense, reste malgré tout trop limitée en cas de crise majeure impactant de larges parties voire la totalité du territoire national.

Compte tenu de l'engagement déjà conséquent des forces (OPEX, Sentinelle, Résilience), le développement à court terme des capacités ne peut être obtenu que par un recours accentué aux réserves. Or, la Garde nationale dispose à l'heure actuelle d'effectifs limités (notamment en termes de spécialistes) et sert dans un cadre légal garantissant une faible disponibilité (de 5 à 30 jours par an[52]). Par conséquent, c'est la question de la place que l'on souhaite donner aux réserves et donc de l'extension de leurs missions et capacités qu'il apparaît primordial de traiter à l'avenir, tant pour lutter contre la pandémie numérique que pour agir face à toute crise d'ampleur sur le territoire national.

[52] Ministère des Armées, *La réserve de cyberdéfense : guide explicatif*, 2020, op. cit.