CYBERMENACES ET SÉCURITÉ NATIONALE

Marc WATIN-AUGOUARD

Directeur du centre de recherche de
l'École des officiers de la gendarmerie nationale
Fondateur du Forum International de la Cybersécurité

En 2008, prenant en compte les conclusions sévères des rapports du député Pierre Lasbordes[1] (2006) et du sénateur Roger Romani[2] (2008), le Livre Blanc sur la défense et la sécurité nationale avait consacré plusieurs développements aux menaces se manifestant dans le cyberespace. Un an auparavant, les systèmes informatiques de l'Estonie avaient fait l'objet d'une attaque massive, premier cas concret rendant plausibles les scénarios élaborés. Dans ce nouveau contexte, le Livre Blanc prônait « le passage d'une stratégie de défense passive à une stratégie de défense active en profondeur, combinant protection intrinsèque des systèmes, surveillance permanente, réaction rapide et action offensive »[3]. Il évoquait, d'une manière très discrète, une capacité de lutte informatique offensive avec « un cadre d'emploi couvrant spécifiquement l'ensemble des actions relevant de la lutte informatique, le développement d'outils spécialisés (armes numériques de réseaux, laboratoire technico-opérationnel, etc.) »[4]. En 2012, le rapport du sénateur Jean-Marie Bockel sur la cyberdéfense[5] souligne les progrès accomplis, notamment grâce à la création en 2009 de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), devenue autorité nationale en matière de sécurité des systèmes d'information, et celle, presque concomitante, du dispositif de cyberdéfense déployé au sein du ministère de la défense[6]. Les avancées se manifestent aussi par la stratégie de cybersécurité, dévoilée, le 15 février 2011, par le gouvernement français[7]. Mais le satisfecit accordé s'accompagne aussi d'une invitation à poursuivre et à intensifier les efforts[8]. Le rapporteur préconise, par ailleurs, une meilleure transparence, tant en

---

[1] Lasbordes P., « La sécurité des systèmes information, un enjeu pour la France », Rapport au Premier ministre, 13 janvier 2006.

[2] Romani R., « La cyberdéfense, un nouvel enjeu de sécurité nationale », Rapport d'information n° 449 (2007-2008) au nom de la Commission des affaires étrangères, de la défense et des forces armées du Sénat.

[3] Livre Blanc sur la défense et la sécurité nationale, éditions Odile Jacob/ La Documentation Française, 2008, p. 168.

[4] *Ibid.*, p. 207.

[5] Bockel J.-M., « La cyberdéfense », Rapport d'information n° 681 (2011-2012) au nom de la Commission des affaires étrangères, de la défense et des forces armées du Sénat.

[6] Création au sein de l'état-major des armées d'EMA-Cyberdéfense et renforcement de la Direction générale pour l'armement (DGA-Maîtrise de l'Information).

[7] Voir site de l'ANSSI, www.ssi.gouv.fr.

[8] Ce que confirme la note « Cybersécurité, l'urgence d'agir », Centre d'Analyse Stratégique n° 234, mars 2013.

ce qui concerne les attaques subies qu'en ce qui concerne la doctrine de cyberdéfense, à l'instar de ce que pratiquent certains états qui ont clairement rendu publique la leur. Le sénateur Bockel invite également à sortir du silence et à afficher sans complexe le développement de capacités offensives.

Un an plus tard, les cybermenaces constituent l'un des traits saillants du nouveau Livre Blanc. Celui-ci s'inscrit dans la continuité du précédent, mais il donne à la politique de cyberdéfense une nouvelle impulsion qui se manifestera à court terme par une croissance de ses moyens humains et matériels. En période de restrictions budgétaires, cet effort témoigne d'un choix prioritaire. En osant désormais parler de stratégie offensive, le Livre Blanc met fin à un tabou. La cyberdéfense, un des piliers de la stratégie de sécurité nationale, voit ainsi son champ s'élargir, ce qui rend plus nécessaire encore la nécessité d'en préciser les contours et la place qu'elle occupe dans une politique plus globale de cybersécurité. Cette cybersécurité est marquée par un continuum défense/sécurité qui exige une coopération de tous les acteurs publics, civils et militaires, mais également un partenariat public/privé pour contribuer à l'élaboration d'un ordre public dans le cyberespace. Cet ordre doit s'appuyer sur un droit dont l'élaboration requiert une démarche au moins européenne et, s'agissant du droit interne, une mise en cohérence de textes aujourd'hui épars.

I. La cyberdéfense, un des piliers de la sécurité nationale

La cyberdéfense, érigée en priorité nationale, est initialement l'objet d'un discours très prudent qui écarte toute notion d'action offensive. L'actualité fait tomber le tabou. La cyberdéfense, « décomplexée », doit s'articuler avec les autres composantes de la cybersécurité face à des menaces inscrites dans un continuum défense/sécurité particulièrement perceptible dans le « champ de l'immatériel ». Ce continuum exige une coopération entre les acteurs publics et privés plus étroite encore que celle que l'on observe dans le monde « matériel ».

A. La fin d'un tabou

Quelques mois après les manifestations spectaculaires des virus Stuxnet (2010) et Flame (2012) et les intrusions au sein des systèmes informatiques de Bercy ou de l'Elysée, notamment à l'occasion de la présidence française du G8 et du G20[9], le nouveau Livre Blanc reconnaît de manière plus explicite les risques liés aux cyberattaques. Par leur ampleur, elles peuvent être qualifiées d'acte de guerre et justifier une riposte offensive.

1. L'ampleur croissante des cyberattaques

Chaque jour, des infrastructures d'importance vitale, civiles ou militaires, font l'objet d'attaques, dont l'ampleur et les conséquences sont croissantes. La vulnérabilité des infrastructures numériques résulte d'une faible protection pouvant être anéantie par des actions parfois simples à mettre en œuvre et peu coûteuses.

[9] Intrusions alors attribuées aux chinois, alors qu'elles sont vraisemblablement le fait de la National Security Agency (NSA).

L'espionnage n'est plus le seul objectif poursuivi par les agresseurs. L'entrave[10] et le sabotage entrent désormais dans leurs modes d'action, comme en témoignent la destruction de près de 1000 centrifugeuses du centre nucléaire de Natanz (Iran, 2010) et la mise hors service de 30.000 ordinateurs du pétrolier saoudien Aramco (2012). Les systèmes de contrôle/commande (SCADA[11]), connectés à Internet, sont particulièrement vulnérables. Le couplage de l'informatique de gestion et de l'informatique de production[12] est source d'économies, mais plus propice aux attaques[13]. Cette fragilité est renforcée avec les usines « intelligentes », dont la connectivité permet une meilleure allocation production/ressources[14]. Il en est de même s'agissant des réseaux d'électricité « intelligents » (*smart grid*).

2. *Les cyberattaques les plus graves reconnues comme acte de guerre*

Les cyberattaques, selon le Livre Blanc, « constituent une menace majeure, à forte probabilité et à fort impact potentiel. [...] La récurrence actuelle de ces intrusions, notamment par des états, donne à penser que des informations sont méthodiquement collectées pour rendre possible, dans une situation de conflit, une attaque de grande envergure. Une telle attaque serait susceptible de paralyser des pans entiers de l'activité du pays, de déclencher des catastrophes technologiques ou écologiques et de faire de nombreuses victimes. Elle pourrait donc constituer un véritable acte de guerre »[15]. Aucun texte officiel français n'avait jusqu'alors qualifié certaines attaques « d'acte de guerre ». On sait que tout engagement conventionnel des forces s'accompagne désormais d'une composante cybernétique. C'est la première fois qu'est consacrée par la doctrine l'idée qu'un conflit dans le cyberespace puisse avoir sa propre logique, une cynétique indépendante. Le Livre Blanc ajoute que « les capacités d'identification et d'action offensive sont essentielles pour une riposte éventuelle et proportionnée à l'attaque »[16]. Le tabou est donc brisé! Désormais, la France reconnaît une posture plus active, plus offensive, comme en témoigne le discours de Jean-Yves Le Drian, à Rennes, le 3 juin 2013 : « [...] La capacité informatique offensive, associée à des capacités de renseignement, concourt de façon significative à notre posture de cybersécurité. Elle contribue notamment à caractériser la menace et à identifier son origine. Elle permet, en outre, d'anticiper certaines attaques et de configurer nos moyens de défense en conséquence. La capacité offensive enrichit la palette des options qui sont à la disposition de l'état. Elle comporte elle-même différents stades, qui sont plus ou moins réversibles, plus ou moins discrets, mais toujours proportionnés à l'ampleur et à la gravité de la situation ».

---

[10] Il s'agit notamment des attaques par déni de service (DDOS), à partir de milliers d'ordinateurs « zombies », dont l'attaquant a pris le contrôle pour adresser à la cible autant de requêtes simultanées qui saturent le système. Un réseau des machines infectées (botnet) est ainsi à l'origine de l'attaque subie par la NSA, le 25 octobre 2013.

[11] Supervisory Command And Data Acquisition.

[12] La généralisation du protocole Internet (Internet Protocol) entraîne la connexion de tous les systèmes au même réseau.

[13] Aramco a été victime du code malveillant « Shamoon ». Même isolés les SCADAs demeurent vulnérables, comme en témoigne l'attaque du site de Natanz, partie d'une sclef USB.

[14] Usine 4.0, smart factories.

[15] Livre Blanc sur la défense et la sécurité nationale, 2013, p. 49.

[16] *Ibid.*, p.73.

3. Un volet offensif pour la cyberdéfense

Dans la pratique, la posture française a précédé le verbe. En privé, les responsables reconnaissaient que la cyberdéfense, officiellement défensive, s'appuyait déjà sur des mesures à caractère plus offensif. On ne peut, en effet, caractériser une attaque ou en atténuer les effets sans chercher à accéder aux systèmes qui sont à leur origine, ne serait-ce que pour comprendre les mécanismes et en stopper les effets. Il ne s'agit pas d'actions « préemptives », comme celles engagées par certains états, mais de dispositions techniques s'inscrivant dans la réponse à une attaque informatique, dans un contexte que le droit commun et le droit des conflits armés qualifient de légitime défense.

La cyberdéfense s'inscrit pleinement dans la stratégie de sécurité nationale, car elle prend en compte des menaces se situant dans le haut du spectre. Combinaison de politiques publiques qui ne relèvent pas du seul champ du ministère de la défense, elle est une composante essentielle d'une stratégie de cybersécurité, dont les contours doivent être précisés.

B. Une nécessaire clarification sémantique

Le préfixe cyber est aujourd'hui couramment employé dans le vocabulaire de la défense et de la sécurité: cybersécurité, cybercriminalité, cyberdéfense, etc. Au moment où la France s'engage dans une politique globale et cohérente, une clarification sémantique s'impose.

1. La cybersécurité

Une définition de la cybersécurité est contenue dans la recommandation UIT–T X.1205 de l'Union Internationale des Télécommunications, agence de l'ONU: « On entend par cybersécurité l'ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyber-environnement et les actifs des organisations et des utilisateurs. Les actifs des organisations et des utilisateurs comprennent les dispositifs informatiques connectés, le personnel, l'infrastructure, les applications, les services, les systèmes de télécommunication, et la totalité des informations transmises et/ou stockées dans le cyberenvironnement. La cybersécurité cherche à garantir que les propriétés de sécurité des actifs des organisations et des utilisateurs sont assurées et maintenues par rapport aux risques affectant la sécurité dans le cyberenvironnement. Les objectifs généraux en matière de sécurité sont les suivants : disponibilité, intégrité – qui peut englober l'authenticité et la non-répudiation-confidentialité ».

Plus simple est la définition donnée par l'Autorité Nationale de Sécurité des Systèmes d'Information (ANSSI) : la cybersécurité est un « état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à

des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense ». La cybersécurité, ainsi définie, est le fruit d'une pluralité d'actions, dont la sécurité des systèmes d'information constitue le volet préventif qui relève de l'action quotidienne.

2. La sécurité des systèmes d'information

La sécurité des systèmes d'information (SSI) concerne l'ensemble des acteurs publics et privés (administrations, entreprises, collectivités territoriales, etc.) qui l'appliquent par des mesures d'ordre interne. Plus tournée vers la prévention et la protection, elle relève de la responsabilité de chacun d'eux. Disponibilité, intégrité, confidentialité et traçabilité en sont les quatre piliers. Dans toute entreprise mettant en œuvre une informatique de gestion ou de production un responsable de la sécurité des systèmes d'information (RSSI) met en œuvre la politique de sécurité, sous l'autorité de la direction générale ou du directeur des systèmes d'information (DSI).

Au sein des ministères, les Hauts fonctionnaires de Défense et de Sécurité (HFDS) et les fonctionnaires de SSI (FSSI) exercent cette mission à l'égard de l'ensemble de la chaîne organique. Les collectivités territoriales, quant à elles, et leurs établissements publics développent de plus en plus la fonction SSI, car, ni les unes, ni les autres ne sont épargnés. La sécurité des systèmes d'information se situe donc en amont de toute autre action. C'est à cet échelon que doit s'opérer la détection des attaques et la mise en œuvre des mesures d'urgence pour empêcher leur développement, notamment grâce à une capacité de cyberrésilience. Dans les entreprises les plus sensibles, la sécurité des systèmes d'information est complétée par des mesures plus contraignantes relevant de la cyberdéfense.

3. La cyberdéfense

La cyberdéfense ne saurait être confondue avec la cybersécurité du ministère de la défense. Elle est définie par l'ANSSI comme « l'ensemble des mesures techniques et non-techniques permettant à un état de défendre dans le cyberespace les systèmes d'information jugés essentiels[17] ». Ces systèmes sont notamment mis en œuvre par l'état (administrations, forces armées, etc.) et les opérateurs publics ou privés. Ceux-ci, selon l'article 1332-1 du code de la défense, exploitent ou utilisent des installations d'importance vitale, dont l'indisponibilité risquerait de diminuer de façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation. On en dénombre aujourd'hui 219 (dont 106 civils) relevant de 12 secteurs critiques. La liste de ces opérateurs est classifiée. Comme le soulignent le Livre Blanc et la loi de programmation militaire, les exigences de la cyberdéfense justifient le respect par les opérateurs d'obligations (déclaration d'incidents, contrôles, etc.). Ces obligations s'imposent également aux sous-traitants ou prestataires de service, car ils peuvent être à l'origine de l'introduction de codes malveillants. La cyberdéfense concerne donc de nombreuses entreprises qui relèvent des transports, de l'énergie, de la défense, de la santé, du secteur bancaire, etc. Elle

[17] Tous les systèmes d'un opérateur d'importance vitale ne relèvent pas de la cyberdéfense. Seuls les plus sensibles sont pris en compte, les autres étant protégés au titre de la SSI.

n'est donc pas cantonnée au domaine strictement militaire, même si ce dernier occupe en son sein une place importante.

Étroitement liée à la notion de souveraineté, la cyberdéfense ne porte pas seulement sur la « couche matérielle »[18] et la « couche logicielle »[19] de la cyber-structure. Elle veille aussi à l'intégrité de la « couche sémantique », c'est-à-dire l'ensemble des données. Les affaires d'espionnage, récemment dévoilées[20], mettent en exergue la nécessaire protection des données sensibles. Celles-ci doivent être protégées du « pillage systématique du patrimoine diplomatique, culturel et économique »[21]. Les « menaces avancées et persistantes » constituent une forme d'attaque furtive qui a pour objectif d'espionner ou de voler des données[22]. La souveraineté des données est également affectée par « l'informatique en nuage » (*cloud computing*) qui expatrie le plus souvent leur stockage, avec tous les risques d'atteinte à la confidentialité que cela implique lorsqu'elles ont un caractère sensible. Les hébergeurs sont généralement anglo-saxons... D'où la volonté du gouvernement de favoriser la création de « *clouds souverains*[23] ».

La souveraineté est aussi tributaire du maintien et, si possible, du développement d'un potentiel industriel et de R&D protecteur des intérêts nationaux[24]. La cyberdéfense n'est pas seulement d'ordre technique ou juridique ; elle s'appuie aussi sur une posture politique et diplomatique. Elle est liée à la lutte contre la cybercriminalité, car les actes qui lui portent atteinte sont généralement des infractions prévues et réprimées par la loi pénale.

4. La lutte contre la cybercriminalité

La troisième composante de la cybersécurité est la lutte contre la cybercriminalité. Il n'existe pas de définition universelle de la cybercriminalité, y compris dans la Convention du Conseil de l'Europe sur la cybercriminalité[25]. En France, la doctrine s'accorde sur une classification tripartite des actes qui en relèvent. La cybercriminalité regroupe:

- Les infractions qui visent les technologies de l'information et de la communication, notamment les systèmes de traitement automatisés de données (STAD) et, d'une manière générale, tous les systèmes connectés qui échangent des

[18] Le *hardware* : ordinateurs, routeurs, câbles, satellites, etc.
[19] Le *software* comprend notamment les systèmes d'exploitatioon, les utilitaires.
[20] Programme PRISM de la National Security Agency (NSA), révélé à la presse, en 2013, par Edward Snowden, ex-consultant de la NSA.
[21] Bocke J.-M., *La France et la cyberdéfense*, Administration, n° 239 sept-oct 2013, p. 68.
[22] *Advanced Persistent Threat* (APT). L'attaque qui a visé le ministère des finances à Bercy a duré deux ans et a porté sur 150 ordinateurs. Elle a nécessité l'intervention de cinquante experts en 3x8 pendant quatre mois. Le délai entre le début d'une attaque APT et sa découverte est en moyenne de 416 jours...
[23] « *Numergy* » conçu par SFR et Bull, « *Cloudwatt* » par Orange et Thalès. Ces « clouds » ont bénéficié du soutien des « Investissements d'avenir ».
[24] C'est l'un des objectifs du Comité de la filière industrielle de sécurité (CoFIS), installé par le Premier ministre, le 23 octobre 2013.
[25] Celle-ci distingue cependant quatre catégories : les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques, les infractions informatiques (falsification, fraude), les infractions de contenu (pornographie enfantine) et les atteintes à la propriété intellectuelle et aux droits connexes.

données (notamment des données à caractère personnel). Ces infractions n'existeraient pas sans le développement des technologies numériques.

- Les infractions de « contenu » qui répriment la détention, l'échange, le transfert, la diffusion, etc. de messages illicites (pédopornographie, incitation à la haine raciale, diffamation, propagande terroriste, etc.) véhiculés par les technologies de l'information et de la communication[26]. De telles infractions peuvent être commises en dehors du cyberespace, mais elles bénéficient avec internet et, en particulier, grâce au développement des réseaux sociaux, d'un exceptionnel vecteur d'amplification. Ainsi une information peut atteindre plusieurs millions d'internautes en quelques secondes et connaître une diffusion exponentielle difficile à maîtriser.

- Les infractions facilitées par les technologies numériques, en particulier celles qui relèvent de la délinquance économique et financière (fraude, escroquerie, blanchiment, atteintes à la propriété intellectuelle dont la contrefaçon, monnaie virtuelles, etc.). Internet est un facilitateur sans égal de trafics ou d'escroqueries.

Toutes les infractions ne sont pas de nature à mettre en cause la sécurité nationale. La cyberdélinquance, motivée le plus souvent par l'appât du gain, relève de ce que l'on nomme « sécurité quotidienne » sans jamais en préciser les contours. En revanche, toutes les atteintes entrant dans le champ de la cyberdéfense sont des infractions pénales.

5. *Lutte contre la cybercriminalité et cyberdéfense*

Des interprétations opposent parfois la lutte contre la cybercriminalité à la cyberdéfense alors que les deux se composent. Dans son rapport précité, le sénateur Bockel dresse une frontière entre cyberdéfense et cybercriminalité: « la cyberdéfense, écrit-il, se distingue en particulier de la lutte contre la cybercriminalité [...], volontairement écartée de la réflexion pour se concentrer sur les attaques informatiques susceptibles de porter atteinte aux intérêts fondamentaux de la Nation [...] »[27]. Mais ces attaques constituent bien des infractions (espionnage, sabotage, etc.), prévues et réprimées par le livre IV du code pénal, consacré notamment aux intérêts fondamentaux de la Nation et au terrorisme. En outre, depuis la loi « Godfrain »[28], les atteintes aux systèmes de traitement automatisés de données (STAD), les vols, destructions, modifications de données sont passibles de sanctions pénales[29]. Sauf dans l'hypothèse d'un conflit armé, les attaques entrant dans le champ de la cyberdéfense sont des infractions qui relèvent de la compétence de la justice et des services spécialisés de la police et de la gendarmerie. Il existe donc un continuum au sein de la cybersécurité. Les champs de la cybercriminalité et de la cyberdéfense s'interpénètrent. La première ne s'arrête pas là où commence la seconde. La cyberdéfense, comme la lutte contre la cybercriminalité, repose sur la

[26] Les sénateurs ont introduit dans le projet de loi pour l'égalité entre les femmes et les hommes une nouvelle infraction : le fait, par tout moyen de soumettre une personne à des humiliations ou à des intimidations répétées, ou de porter atteinte de façon répétée à sa vie privée (futur art. 222-14-3-1 du code pénal). Cette nouvelle infraction est motivée par les débordements observés sur les réseaux sociaux.

[27] Bockel J.-M., « La cyberdéfense ». Rapport d'information n° 681 (2011-2012) au nom de la Commission des affaires étrangères, de la défense et des forces armées du Sénat.

[28] Loi n° 88-19 du 5 janvier 1988 sur la fraude informatique.

[29] Les infractions définies par la loi « Godfrain » peuvent être des actes de terrorisme au sens de l'article 421-1, 2° du Code pénal.

veille des réseaux, la détection des actes illicites, leur traçabilité, la mis en évidence de la preuve numérique. La R&D au profit de l'une sert les intérêts de l'autre. Par exemple, toute avancée dans la traçabilité des attaques permet aux enquêteurs de remonter vers les auteurs de l'infraction. La symbiose entre la lutte contre la cybercriminalité et la cyberdéfense illustre parfaitement le continuum défense/sécurité qui se manifeste de manière éclatante dans le cyberespace.

C. Un continuum défense/sécurité

Le continuum caractérise l'absence de rupture entre le champ de la défense et celui de la sécurité, entre le temps de paix et le temps de guerre. « L'ordinaire et l'extraordinaire » sont intriqués dans le cyberespace. Le recours à la guerre y est très peu probable, car la furtivité de l'agression, grâce à son anonymat, est le premier effet recherché par son auteur.

1. « l'ordinaire et l'extraordinaire » intriqués

Le continuum défense-sécurité est particulièrement affirmé dans le cyberespace, ne serait-ce qu'en raison de l'absence de frontières. Il n'y a pas de distinction entre un « champ de bataille » et des « quartiers sensibles », entre le territoire national et l'étranger[30]. S'il est vrai que les cyberdélinquants poursuivent des objectifs différents de ceux des cyberterroristes ou des « cyberguerriers », ils utilisent parfois les mêmes armes, empruntent les mêmes réseaux. Par exemple, une attaque par déni de service[31] peut être le fait de délinquants qui cherchent un profit en opérant un chantage sur un opérateur de commerce en ligne, d'entreprises qui veulent affaiblir un concurrent, de terroristes qui veulent désorganiser les secours simultanément à un attentat[32], ou le fait d'agresseurs qui veulent affaiblir ou paralyser le fonctionnement d'un état. Les fournisseurs d'ordinateurs « zombies » n'ont pas d'état d'âme ; ils peuvent louer leurs services aux uns comme aux autres. En 2010, le FBI, la garde civile espagnole et la police criminelle slovène ont mis un terme aux agissements d'un groupe à l'origine d'un réseau d'ordinateurs piratés baptisé *Mariposa*. Selon les estimations, entre 8 à 12 millions d'ordinateurs étaient sous leur contrôle. Ce parc, loué temporairement sur internet, pouvait servir à adresser des *pourriels*, à récupérer des données bancaires, à conduire des cyberattaques à des fins crapuleuses ou politiques. Les marchés noirs organisés sur internet[33] servent aussi bien aux réseaux criminels qu'aux terroristes ou aux « guerriers ». Seul le mobile permet de différencier les actions conduites par des prédateurs « multicartes »[34]. La qualification d'une attaque dépend aussi de son

[30] Sauf en ce qui concerne l'application de la loi pénale.

[31] Une attaque par déni de service fait appel à de très nombreux ordinateurs « zombies », sous contrôle des attaquants, qui vont saturer la cible par des interrogations simultanées, empêchant ainsi tout usage normal du système informatique.

[32] Par exemple, en attaquant le SCADAs qui commandent les numéros d'urgence, la signalisation routière, les hôpitaux, ajoutant la désorganisation à la terreur.

[33] Les marchés noirs de la cybercriminalité, étude, Compagnie Européenne d'Intelligence Stratégique (CEIS), 2011.Les black markets utilisent des monnaies virtuelles et facilitent le financement d'activités illégales.

[34] La même remarque peut être faite à propos de l'espionnage, de l'ingénierie sociale, de la diffusion de contenus de nature à troubler l'ordre public, etc.

intensité, de sa complexité, de la nature de la cible. La frontière entre ce qui relève de « l'ordinaire », la sécurité quotidienne, et de « l'extraordinaire », la cyberdéfense, est particulièrement poreuse du fait de la connexité des actions. Une cybertattaque peut être précédée, suivie ou accompagnée d'autres infractions (atteinte à la réputation des autorités civiles et militaires, incitation à la haine, propagande terroriste, fraude, blanchiment d'argent, usurpation d'identité, etc.). Les investigations menées dans le cadre d'une enquête judiciaire peuvent mettre en évidence les éléments matériels d'une attaque relevant de la cyberdéfense et inversement. Le renseignement « d'intérêt cyber » ne peut donc être compartimenté. Dans l'espace réel, le continuum rapproche la communauté policière de la communauté militaire. Dans le cyberespace, la « policiarisation » de l'action militaire se confirme.

2. *L'improbable rupture du continuum*

Une cyberattaque relevant de la cyberdéfense constitue, comme on l'a dit supra, une infraction prévue et réprimée par le code pénal. Ainsi en est-il tant que ne s'applique pas le droit des conflits armés (droit de La Haye, Convention de Genève et ses protocoles additionnels, etc.). Depuis les attaques en Estonie (2007) et en Géorgie (2008), les médias, comme certains militaires, évoquent une possible « cyberguerre ». Il est aujourd'hui admis que tout conflit a une composante cyber qui précède ou accompagne l'engagement conventionnel des forces en vue d'affaiblir ou de neutraliser les capacités de l'adversaire. Dans cette hypothèse, le droit des conflits armés trouve son application[35]. Lors du conflit avec la Géorgie, les forces armées russes ont ainsi « préparé le terrain » avant d'engager les blindés et l'aviation. Dans le cas de l'Estonie, la situation est plus complexe : il n'y a jamais eu signature des attaques, notamment parce qu'il n'y a pas eu d'engagement conventionnel trahissant l'identité de l'agresseur[36]. L'hypothèse d'une guerre autonome dans le cyberespace est très peu probable. Pour qu'il y ait une guerre, il faut un adversaire étatique identifié. Or, la recherche de l'anonymat est la première précaution de l'agresseur. Ce dernier, pour garantir l'opacité de son action, a recours à des « tiers attaquants » (mafias, officines, groupes criminels, groupes paramilitaires, etc.), dont il peut se désolidariser en cas de soupçon. La guerre renvoie à la notion d'agression armée qui doit atteindre une certaine ampleur et avoir des conséquences physiques (destructions) et humaines (tués et blessés). En Estonie, aucune perte humaine n'a été déplorée. En Iran, des destructions ont été constatées, mais elles ont été sans conséquence pour les personnes.

Pour l'heure, faute de pouvoir, pour les motifs précités, qualifier une attaque cybernétique d'agression armée, seules les actions connexes à un conflit conventionnel peuvent entrer dans le champ de la cyberguerre. Dans toutes les

[35] À condition qu'il soit adapté, notamment en ce qui concerne la légitime défense, le respect de la neutralité, le non-recours à la perfidie, la protection des civils et des sites inviolables (hôpitaux, écoles, etc.). Le Manuel de Tallinn, rédigé par des experts de l'OTAN, tente cette transposition, mais il n'a aucune valeur normative.

[36] Cette attaque a fait suite au déplacement d'un monument érigé en 1947 sur la colline de Tonismäe, à Tallinn, en mémoire des soldats soviétiques de la Seconde Guerre mondiale. La Russie a, bien entendu, été suspectée sans que des preuves formelles soient apportées.

autres hypothèses, le droit commun s'applique[37]. Il n'y a pas de discontinuum juridique. Les attaques sont des infractions justifiant une étroite coopération entre tous les acteurs de la cybersécurité.

3. *Un nécessaire renforcement de la coopération entre tous les acteurs publics ou privés*

La cyberdéfense ne commence donc pas là où s'arrête la lutte contre la cybercriminalité. La sécurité du cyberespace n'est pas sécable, mais est tributaire d'une coopération permanente entre magistrats, policiers, gendarmes, militaires des armées, opérateurs, fournisseurs d'accès, etc.

La coopération concerne d'abord les acteurs régaliens. L'ANSSI, la composante cyberdéfense de l'état-major des armées, les services de police et les unités de gendarmerie, les services de renseignement etc. ont l'obligation de coopérer, car la complexité des attaques dans le cyberespace nécessite la mobilisation de toutes les compétences, une plus grande transversalité. Le pôle « cyberdéfense » sort particulièrement renforcé grâce au Livre Blanc et à la loi de programmation militaire. L'ANSSI devrait voir ses effectifs portés à 500, à l'horizon 2015. Ceux d'EMA-cyber défense devraient atteindre la cible de 400, tandis qu'un volume similaire est prévu pour DGA-Maîtrise de l'information. La récente colocalisation du Centre Opérationnel de la Sécurité des Systèmes d'Information (COSSI) et du Centre d'Analyse de Lutte Informatique Défensive (CALID), témoigne d'une recherche de synergies[38]. La gendarmerie nationale est présente au sein du CALID ; elle participe également à la réserve cyberdéfense[39]. Le pôle « lutte contre la cybercriminalité », quant à lui doit être mieux structuré. Les services de police[40], de gendarmerie[41] et de douanes[42] ont développé leurs services spécialisés depuis près de quinze ans. La Justice, quant à elle, doit être mieux organisée, car la cybercriminalité est entrée dans les prétoires avec un contentieux croissant en volume et en complexité. Comme le propose Jean-Marie Bockel dans son rapport précité, il est aujourd'hui indispensable de créer une ou plusieurs juridictions spécialisées, à l'instar de ce qui existe pour le terrorisme, la criminalité organisée, la santé publique, la mer. Il convient de définir également une politique pénale qui fait encore défaut. Le groupe de travail interministériel, dirigé par le procureur général Marc Robert, devrait rendre son rapport avant la fin du premier trimeste 2014. La

[37] La reconnaissance par le législateur de l'irresponsabilité pénale des acteurs de la cybersécurité, agissant contrairement aux dispositions de la loi « Godfrain », est bien la preuve que l'action des services spécialisés s'inscrit principalement dans le droit commun (art. L.2321-1 Code de la défense).

[38] Le COSSI relève de l'ANSSI, tandis que le CALID est une entité d'EMA- cyberdéfense.

[39] Réserve composée de réservistes citoyens et de réservistes opérationnels spécialistes dans les domaines liés au cyberespace. La gendarmerie anime trois des cinq pôles régionaux expérimentaux : Nord-Pas-de-Calais, Alsace, Rhône-Alpes.

[40] Le dispositif de la police nationale comprend l'Office central de lutte contre les infractions liées aux technologies de l'information et de la communication (OCLCTIC) de la Direction centrale de la police judiciaire, la Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI), de la Préfecture de police, 260 investigateurs en cybercriminalité (ICC)

[41] La gendarmerie nationale dispose d'un plateau d'investigation Cybercriminalité et Analyses Numériques (PICyAN) qui regroupe les moyens dédiés de l'Institut de Recherche Criminelle de la Gendarmerie (IRCGN) et du Service Technique de Recherche Judiciaire et de Documentation (STRJD). A l'échelon national, 60 experts, 260 enquêteurs NTECH et 1000 correspondants NTECH constituent la communauté des « cybergendarmes ».

[42] Cyberdouane est un service de la Direction nationale des recherches et enquêtes douanières (DNRED).

cohérence du pôle « lutte contre la cybercriminalité » est essentielle si l'on veut mieux articuler son action avec celui de la cyberdéfense. Ajoutons que la coopération entre les services de renseignement doit être accentuée, notamment dans le domaine technique, compte tenu de l'importance des investissements.

La coopération ne se limite pas aux acteurs régaliens. La cybersécurité repose aussi sur l'action des acteurs privés, opérateurs, intégrateurs, prestataires de services, etc. Il existe un secteur privé de la cybersécurité qu'il faut conforter. Sans doute conviendrait de le reconnaître et de l'organiser par une loi similaire à celle du 12 juillet 1983, relative aux activités privées de sécurité. Ces acteurs sont, dans une certaine mesure, des collaborateurs du service public. Il importe de définir des critères de confiance, sanctionnés par une labellisation. Dans le domaine de la cybersécurité, la part régalienne de l'offre de sécurité est minoritaire. Cette convergence entre le public et le privé ne peut s'envisager sans une politique industrielle qui fasse émerger des « géants », si possibles français, au moins européens, car la question de la souveraineté est essentielle, sauf à accepter une domination américaine ou chinoise. Cette souveraineté est tributaire d'une capacité de recherche et développement qui garantisse une meilleure indépendance au regard des innovations technologiques. Elle repose également sur un effort en matière de formation, car les acteurs publics, comme les acteurs privés sont aujourd'hui confrontés à une pénurie en matière de ressources humaines dans les domaines liés aux technologies numériques[43].

La cybersécurité est en mouvement. Son architecture devrait encore évoluer dans les années à venir, ne serait-ce que parce que des efforts supplémentaires seront nécessaires. Le droit doit accompagner cette profonde mutation.

II. L'adaptation du droit aux exigences de la cybersécurité

Tout espace conquis par l'homme est un vecteur de liberté, d'échanges, de croissance, de développement culturel, etc. Mais il est aussi très rapidement la proie des prédateurs. Le droit est créateur d'ordre public : il autorise, oblige, interdit, encadre, régule. Sa construction témoigne de la prise de conscience des enjeux. Dans le cyberespace, la sécurité, singulièrement mise à mal depuis 2007, appelle l'élaboration d'un droit en phase avec les mutations technologiques. La conquête des espaces par l'homme s'accompagne toujours d'une évolution du droit international et du droit interne. Parfois, la maturation est lente, comme en témoignent les quatre siècles qui séparent Grotius de la Convention des Nations Unies sur le droit de la mer de Montego Bay (1982). S'agissant du cyberespace, les mutations technologiques et sociologiques sont si rapides qu'il est nécessaire d'ajuster en permanence et sans délai le corpus juridique qui le régit. De la protection de l'individu vis-à-vis d'un « Big Brother » à l'émergence d'un droit de la cyberdéfense, trente cinq ans se sont écoulés. C'est peu, au regard de l'histoire de l'humanité, mais c'est beaucoup si l'on prend en compte le rythme de la reconfiguration d'une société désormais structurée par le « tout numérique ». Le cyberespace, par construction sans frontière, devrait reposer sur un droit conventionnel universel. Force est de reconnaître que la communauté internationale est partagée sur la conception de sa sécurité. Malgré les difficultés, le droit du cyberespace progresse en Europe et en France. La publication,

[43] L'Europe pourrait connaître un déficit de compétences de l'ordre de 900.000 emplois en 2016.

en février 2013, par l'Union européenne d'une stratégie de cybersécurité et celle, plus récente, d'une directive relative aux attaques contre les systèmes d'information constituent une avancée, même si elle est limitée dans son champ géographique. Côté français, la loi de programmation militaire vient compléter un corpus juridique, souvent très en phase avec l'évolution des pratiques dans le cyberespace, en donnant un cadre juridique à la cyberdéfense.

A. Un engagement plus résolu de l'Europe

Les pionniers du cyberespace étaient partisans d'une liberté absolue. Ils ignoraient sans doute que cet espace, créé par l'homme, serait, lui aussi, investi par les prédateurs de toute nature : délinquants, terroristes, mercenaires, guerriers. La liberté absolue, c'est la loi du plus fort. Une régulation est indispensable pour établir un ordre public, équilibre entre sécurité et liberté. Cette régulation a longtemps échappé aux pouvoirs publics, dans la mesure où ces derniers l'ont abandonnée à des organismes privés (ICANN[44], ISOC[45], IETF[46], W3C[47], etc.), relevant pour la plupart du droit américain. Le développement de la cybercriminalité et les attaques mettant en danger la sécurité nationale ont incité la communauté internationale à s'engager dans l'élaboration d'un droit universel. Malheureusement, les initiatives ont connu un succès limité. La Convention du Conseil de l'Europe relative à la lutte contre la cybercriminalité (Budapest, 23 novembre 2001) est le seul traité international qui soit aujourd'hui opérant, malgré le nombre encore restreint des états l'ayant ratifié (40 en octobre 2013). Les efforts de l'ONU en vue de l'élaboration d'une convention sur la cybercriminalité risquent de déboucher sur un compromis *a minima* sur les standards les plus faibles. L'échec de la Conférence mondiale sur les communications internationales, sous l'égide de l'Union Internationale des Télécommunications (Dubaï, décembre 2012) souligne la division des états au regard de la gouvernance d'Internet. Certains (Russie, Chine, etc.) veulent, au titre de la sécurité nationale, contrôler les données qui transitent, d'autres (les pays occidentaux en particulier) entendent préserver la liberté des échanges. Le cyberespace est sans doute celui au sein duquel les questions de souveraineté sont aujourd'hui les plus exacerbées, ce qui explique l'absence de consensus. Dans ce contexte, il est nécessaire que l'Europe, au moins, adopte une posture unitaire.

Depuis le Conseil de Tampere (oct.1999), le principe du rapprochement des droits internes dans le domaine de la cybercriminalité est acquis. La création, en 2004, de l'ENISA (European Union Agency for Network and Information Security), dont les pouvoirs ont été renforcés après le vote du parlement du 16 avril 2013, la décision cadre 2005/222/JAI, la communication 2007/267« vers une politique générale en matière de lutte contre la cybercriminalité, la création au sein d'Europol de EC3 (European Cybercrime Center) illustrent la construction d'une posture européenne de cybersécurité. La directive 2013/40/UE du Parlement européen et du

[44] Internet Corporation for Assigned Names and Number, association de droit californien qui administre les noms de domaine (DNS) : .fr, .com, .org, .net, etc.

[45] Internet Society, association de droit américain qui promeut et coordonne le développement des techniques relatives à internet.

[46] Internet Engineering Task Force, liée à l'ISOC, regroupe des ingénieurs et des chercheurs (80 % sont américains...) chargés de faire évoluer les standards. En son sein, l'Internet Architecture Board est chargé de l'évolution de l'architecture du Net.

[47] World Web Consortium qui veille à la compatibilité des technologies utilisées sur le Web.

Conseil en date du 12 août 2013, relative aux attaques contre les systèmes d'information en est l'étape la plus récente. Cette directive doit être transposée dans les droits nationaux avant le 4 septembre 2015. Par rapport à la décision cadre de 2005 qu'elle remplace, la directive ajoute notamment des dispositions relatives à la protection des infrastructures critiques. C'est précisément l'un des volets de la loi de programmation militaire en cours d'examen au Parlement.

B. Le renforcement du corpus juridique national

La loi de programmation militaire[48] contient plusieurs articles, enrichissant notamment le code de la défense et relatifs à la lutte contre les cybermenaces. Les puristes s'étonneront de l'insertion de dispositions non directement liées à l'objet principal de loi : la programmation des moyens des armées. Les pragmatiques s'en féliciteront, car le calendrier législatif n'aurait pas permis un examen séparé avant l'été 2014…Or, il y a urgence à renforcer la politique de cybersécurité, notamment au bénéfice des infrastructures critiques gérées par des opérateurs d'importance vitale (OIV). Il s'agit, selon l'actuel article L.1332-1 du code de la défense d'opérateurs « dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ». Plusieurs dispositions retiennent l'attention.

Le texte, tout d'abord, conforte l'architecture sommitale de cybersécurité. Il attribue au Premier ministre la responsabilité de définir et de coordonner l'action gouvernementale, dans le cadre de la stratégie de sécurité nationale et de la politique de défense (art. 21). Sans doute cet article est-il redondant par rapport aux attributions générales que confère l'article 21 de la Constitution au chef du gouvernement, mais il n'est pas inutile de rappeler qu'une politique de cybersécurité est par essence interministérielle. En outre, en précisant que le Premier ministre dispose de l'autorité nationale de sécurité des systèmes d'information (ANSSI), l'article 21 (art. L.2321-1 du code de la défense), donne une consécration législative à cette institution récente, créée par un simple décret[49].

La loi donne une base légale à l'action des services appelés à lutter contre des attaques (art. L.2321-2 du code de la défense). Aujourd'hui, la loi Godfrain, (art 323-1 et s. du code pénal) réprime les atteintes aux systèmes de traitement automatisé de données et la détention d'équipements permettant de les réaliser. Cette loi, particulièrement novatrice en 1988, n'avait pas imaginé la nécessité de parer les cyberattaques par des actions « offensives ». Il faut, en particulier, accéder au système informatique de l'attaquant, aux données qu'il contient. On notera que cette autorisation donnée par la loi se limite aux opérations menées « en réponse à une attaque », ce qui exclut toute action préemptive. Le droit français ne s'écarte pas de la légitime défense. À une époque marquée par une judiciarisation parfois excessive, il est nécessaire de protéger les acteurs de la cyberdéfense contre tout risque pénal.

La sécurité juridique des prestataires de service et des industriels est également mieux garantie grâce à une modification de l'article 323-3-1 du code pénal qui leur permet d'exercer une activité de recherche ou de développement de produits ou de service de sécurité informatique, actions aujourd'hui proscrites par le

[48] La loi de programmation militaire est en cours d'examen au moment où cet article est rédigé. Seuls sont évoqués les éléments connus au moment de sa remise à l'éditeur.
[49] Décret n° 2009-834 du 7 juillet 2009

code pénal, sauf « motif légitime ». Cette mesure est de nature à lever les incertitudes qui pèsent sur les acteurs de la sécurité informatique, au moment où l'on veut développer une politique industrielle ambitieuse.

Le texte clarifie enfin les relations entre les pouvoirs publics et les opérateurs d'importance vitale. L'article 22 du projet introduit six articles dans le code de la défense (art. L.1332-6-1 et s.), relatifs aux pouvoirs du Premier ministre à l'égard des opérateurs publics et privés qui relèvent de secteurs critiques au regard de la sécurité nationale. Celui-ci fixe les règles de sécurité, en fait contrôler l'exécution par des audits. Le non-respect des obligations imposées par la loi, notamment celle de notifier les incidents, peut entraîner des sanctions pénales visant les personnes physiques comme les personnes morales. Les pouvoirs du Premier ministre sont très étendus en cas de crise informatique majeure. Il peut alors décider des mesures que les opérateurs doivent mettre en œuvre, par exemple la déconnexion d'un réseau. La loi de programmation militaire instaure ainsi une nouvelle police administrative spéciale relevant du Premier ministre. Le corpus juridique de la cybersécurité, régulièrement enrichi par les lois, couvre désormais l'ensemble du spectre allant de la cyberdélinquance à la cyberdéfense.

C. Une indispensable clarification du corpus juridique

Tout en se félicitant des progrès réalisés, on doit dresser un double constat: une dispersion du droit du cyberespace contrariant une approche globale et l'absence d'un socle de référence commun.

1. Un droit dispersé

Le droit national qui régit le cyberespace est aujourd'hui dispersé dans de nombreux codes : code pénal, code de procédure pénale, code de la défense, code de la sécurité intérieure, code des postes et des communications électroniques, code monétaire et financier, code de la propriété intellectuelle, etc. Le sénateur Jean-Marie Bockel s'en plaignait dans son rapport sur la cyberdéfense (juillet 2012). Cette dispersion peut s'expliquer par la spécificité des matières concernées, mais elle nuit à la compréhension d'ensemble d'une priorité nationale s'inscrivant dans le continuum défense-sécurité. Ainsi, en cinq articles, la loi de programmation militaire impacte quatre codes... Un code de la cybersécurité serait le bienvenu !

2. Un socle de référence à géométrie variable

Le second constat appelle une mise en cohérence des textes. La stratégie de sécurité nationale,

dont relève évidemment la cybersécurité dans ses implications les plus sensibles, est définie par les items énoncés à l'article L. 1111-1 du code de la défense : vie de la Nation, intégrité du territoire, permanence des institutions de la République, protection de la population. Le code pénal, quant à lui, procède à une énumération plus complète pour définir les atteintes aux intérêts fondamentaux de la Nation. L'article 410 du Code pénal fait ainsi référence à l'intégrité du territoire, la sécurité du territoire, la forme républicaine des institutions, la sauvegarde de la population en France et à l'étranger, aux moyens de la défense et de la diplomatie, à l'équilibre du milieu naturel et de l'environnement, aux éléments essentiels du

potentiel scientifique et économique et au patrimoine culturel. Enfin, pour qualifier les opérateurs d'importance vitale ou justifier les mesures de cyberdéfense prévues par la loi de programmation militaire, la loi invoque les atteintes au « potentiel de guerre ou économique, à la sécurité ou à la capacité de survie de la Nation », ce qui ne recouvre ni le champ des intérêts fondamentaux de la Nation, ni celui de la sécurité nationale. Doit-on en déduire que les intérêts fondamentaux de la Nation dépassent le champ de la sécurité nationale ou que les mesures de cyberdéfense ne concernent pas tous les domaines couverts par les intérêts fondamentaux de la Nation ? Assurément non ! Une telle interprétation serait réductrice. Il serait donc opportun d'harmoniser notre droit en prenant comme référence unique les « intérêts fondamentaux de la Nation ». C'est d'ailleurs ce que la loi de programmation militaire réalise pour le code de la sécurité intérieure, s'agissant des traitements informatisés mis en œuvre par les services de renseignement[50]. Cet alignement sur les intérêts fondamentaux de la Nation serait d'autant plus logique et légitime que ces intérêts ont une valeur constitutionnelle[51].

***

Seul espace entièrement créé par l'homme, le cyberespace est, comme tous les autres, porteur de liberté, de richesses, de croissance, mais il est aussi l'objet de convoitises de la part des prédateurs. Ces derniers, délinquants, terroristes, mercenaires, guerriers, ont compris que le rapport risques/profits leur est plus que jamais favorable. Nul besoin d'être puissant pour faire du fort un faible et du faible un fort. Dans ce contexte, notre société, désormais modelée par le « tout numérique », ne peut laisser le champ libre aux pirates, aux bandits « des grands chemins de l'internet ». La prise de conscience a été lente. Désormais, il faut accélérer le mouvement. Nous n'avons pas le choix ! Soyons-en conscients : nous ne vivons pas une évolution, ni une révolution, mais une métamorphose de notre société ! La chrysalide devient papillon ! Les modèles, organisations, modes d'action, qui ont prouvé leur efficacité dans le passé, sont désormais obsolètes. Si nous ne sommes pas au rendez-vous, nous serons une « colonie du numérique », pour reprendre le titre d'un récent rapport sénatorial[52]. Pire !, nous serons les « esclaves du numérique ». Cet impératif résulte du constat contemporain, mais il doit tenir compte de ce que nous réserve un avenir proche avec notamment l'interconnexion des objets, l'inscription de chaque individu dans une « bulle informationnelle » qui agrègera l'ensemble des données à caractère personnel. Tout cela sera possible car le nombre d'adresses IP (internet protocol) permettant les connexions va passer de 4,3 milliards à 340 milliards de milliards de milliards de milliards. Chaque grain de

[50] Art. L.232-2 du code de la sécurité intérieure.

[51] Les intérêts fondamentaux de la Nation réaffirmés au sein de la Constitution à la faveur de la loi constitutionnelle n° 2005-205 du 1er mars 2005 relative à la Charte de l'environnement : le peuple français considère « que la préservation de l'environnement doit être recherchée au même titre que les autres intérêts fondamentaux de la Nation ». Par ailleurs le Conseil constitutionnel, dans sa décision CC n° 2011-192 QPC du 10 novembre 2011 rappelle les « exigences constitutionnelles inhérentes à la sauvegarde des intérêts fondamentaux de la Nation : « Le secret de la défense nationale participe de la sauvegarde des intérêts fondamentaux de la Nation, réaffirmée par la Charte de l'environnement, au nombre desquels figurent l'indépendance de la Nation et l'intégrité du territoire ».

[52] Morin Desailly C., « L'Union européenne, colonie du monde numérique », rapport d'information fait au nom de la commission des affaires européennes n° 443 (2012-2013) du 20 mars 2013.

sable du désert pourrait ainsi avoir une adresse…Sous peu, sera posée en des termes inédits la question de l'identité des individus, de la compétitivité du secteur économique et de la souveraineté de l'état. La pire atteinte à la sécurité nationale serait de ne pas être en mesure de faire face aux nouveaux enjeux du cyberespace.

Des items à harmoniser

Sécurité nationale	**Intérêts fondamentaux de la Nation**	**Cyberdéfense**
Ref : Art L. 1111-1 du code de la défense	Ref : Art 410 du code pénal	Ref : Art. L2321-2 du code de la défense
Vie de la Nation		Capacité de survie de la Nation
	Indépendance	
Intégrité du territoire	Intégrité du territoire	
	Sécurité du territoire	Sécurité de la Nation
Permanence des institutions de la République	Forme républicaine des institutions	
Protection de la population	Sauvegarde de la population en France et à l'étranger	
	Moyens de la défense et de la diplomatie	Potentiel de guerre
	Équilibre du milieu naturel et de l'environnement	
	Éléments essentiels du potentiel scientifique et économique	Potentiel économique
	Patrimoine culturel	