

Au Sommaire



CYBERGUERRE

- La guerre numérique a commencé :
Entretien avec Nicolas Arpagian 30

GÉOPOLITIQUE

- 2009, année du retour de la Perse ?
par Ardavan Amir-Aslani 18

COMMUNICATION D'INFLUENCE

- De la "Realpolitik"
à la "Real Communication" 22

CRIMINALITÉ FINANCIÈRE

- Crise mondiale : comment gérer
les contradictions dans le domaine
bancaire et financier ? 50
- TRACFIN : la déclaration de soupçons,
une mission de service public 55

L'OBSERVATOIRE DU MONDE TURC

- Démocrates et conservateurs : la révolution
idéologique des islamistes turcs 58

DÉFENSE

- Propagande et opérations psychologiques :
mission des forces spéciales ? 62

CHRONIQUES

- Verbatim 2
- Lectures stratégiques 68
- Confidentiels de Roland Jacquard 70

L'implication
de la Gendarmerie
dans l'Intelligence
économique
au niveau
territorial :

enjeux
et perspectives

*Les Cahiers
de la Compétitivité et de
la Sécurité Économiques*

*en partenariat avec
L'IERSE*

La Lettre

SENTINEL

ANALYSES & SOLUTIONS

LETTRE DE DÉCRYPTAGE DES ENJEUX STRATÉGIQUES ET DES MENACES CONTEMPORAINES

Le retour de la France dans l'OTAN :



- **Fausse raisons
et vraies conséquences** P. 4
- **Le Général face à l'OTAN :
une analyse toujours actuelle** P. 13

De la "Realpolitik" à la "Real Communication"



Retour au réel :
la crise va obliger
les entreprises
à communiquer
autrement

P. 22



La guerre numérique a commencé

Entretien avec Nicolas Arpagian, auteur de "La Cyberguerre"



Journaliste, rédacteur en chef de la revue Prospective Stratégique, coordonnateur des enseignements « Stratégies d'influence & Lobbying » à l'IERSE, Nicolas Arpagian a déjà publié aux Editions Dalloz, en 2007 « Liberté, Egalité... Sécurité » et en 2008 « Pour une stratégie globale de sécurité nationale » cosigné avec Eric Delbecque. Dans « La Cyberguerre : la guerre numérique a commencé », publié aux Editions Vuibert, il offre une parfaite synthèse pour comprendre les tenants et les aboutissants de cette guerre cybernétique qui s'annonce impitoyable dans une économie et une société où tout est désormais virtuel et numérique. Un ouvrage qui fait prendre conscience de l'importance stratégique d'une cyberguerre qui ne peut plus relever uniquement des seuls techniciens mais exige l'implication plus active, en France et en Europe, de l'ensemble de la sphère politique et militaire.

La Lettre Sentinel : La guerre évolue sans cesse : guerre territoriale, guerre économique, guerre de l'information. Le cyberspace est-il le futur champ de bataille des prochains conflits armés ?

Nicolas Arpagian : Le monde cybernétique est devenu un champ de bataille à part entière mais qui peut également contaminer tous les autres champs de bataille. Le couple de futurologues américains Alvin et Heidi Toffler assimilent les technologies de l'information aux armes de longue portée qui permettent de porter les guerres au-delà des limites du champ de bataille traditionnel : amplifiant à l'échelle planétaire de la Toile de simples conflits locaux, jusque-là restreints géographiquement. Les cyberterritoires constituent désormais, au-delà des champs de bataille traditionnels, des lieux d'affrontements de plus en plus violents et décisifs. Assurément la guerre de l'internet est la guerre que nous ne devons pas perdre, au risque sinon de renoncer pour toujours à des éléments clés de notre indépendance.

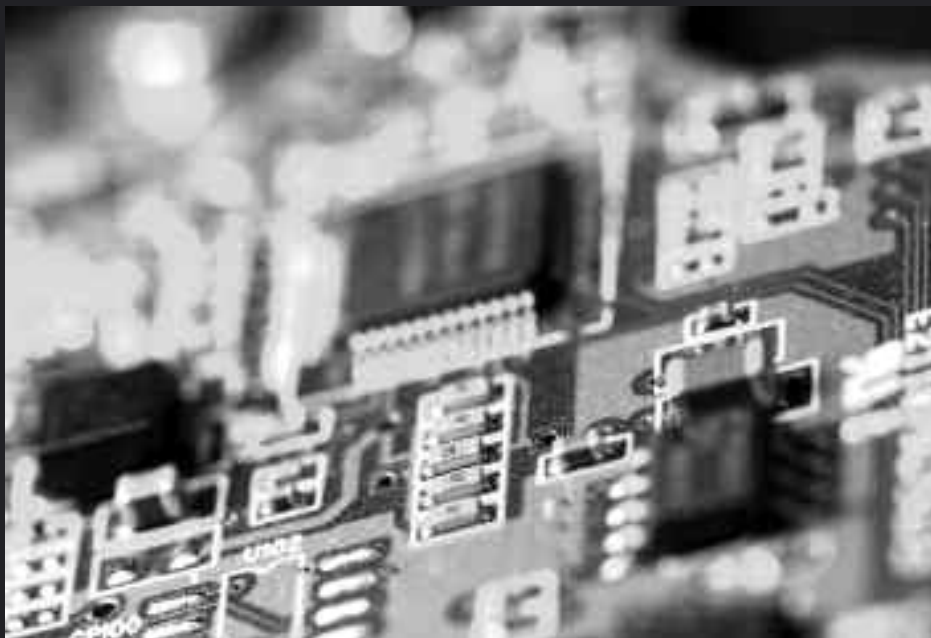
Comment qualifier cette cyberguerre ?

La cyberguerre est à la fois une guerre de l'information et une guerre des réseaux. On peut mener une guerre informationnelle dans le cyberspace comme la France en a été victime lors des JO de Pékin. La guerre de l'information peut se faire aussi par des attaques directement sur

les réseaux pour neutraliser ou détourner les sites gouvernementaux comme ce fut le cas de la Géorgie et de l'Estonie. Il est possible par ailleurs de neutraliser les moyens militaires via les systèmes d'information : l'aviation géorgienne a ainsi été empêchée de décoller. Il aura suffi aux Russes de cibler les réseaux de commandement et de conduite des opérations aériennes pour clouer au sol les dix-huit avions de l'armée de l'air géorgienne. L'exemple géorgien confirme par ailleurs que le cyberattaquant peut aisément mener son offensive sans en avoir les conséquences juridiques. Dans le cas géorgien, les États membres de l'OTAN se sont interrogés pour savoir si ces attaques informatiques pouvaient être assimilées à une intervention militaire classique et entraînant alors l'application de l'article 5 du traité qui prévoit une riposte armée dans l'exercice du droit de légitime défense. Mais bien que tout laissait à penser que l'assaut numérique émanait de la Russie, la Géorgie n'était pas pour autant dans la capacité de la prouver formellement.

Le Livre blanc sur la défense et la sécurité prend-il en compte cette menace de guerre numérique dans sa redéfinition d'une stratégie nationale de sécurité ?

La dimension de la cyberguerre est mise en exergue dans le Livre blanc. Ce qui constitue déjà une rupture car nous étions auparavant dans une logique défensive de pure



constatation des cyberattaques. L'innovation du Livre blanc est d'admettre que la France peut passer à l'offensive. C'est le feu vert du Président de la République et la volonté du Chef d'État-major des armées qui vont permettre de mener des cyberattaques. On s'autorise désormais à utiliser les armes numériques de nos adversaires pour une cyberguerre qui devient un élément de défense et de sécurité à part entière, comme cela se pratique déjà en Europe. Mais il reste à régler la question du respect des lois sur la protection des données tant nationales qu'internationales. Le Spiegel vient ainsi de révéler que le BND, l'équivalent allemand de la DGSE, avait mené 2500 opérations de cyberguerre de manière offensive, c'est-à-dire la prise de contrôle d'un ordinateur à distance : pour soit l'espionner, soit le neutraliser.

Toute offensive militaire aura désormais un volet numérique ?

Incontestablement c'est déjà le cas, le Livre blanc sur la défense et la sécurité nationale énonce très clairement que « dans la mesure où le cyberspace est devenu un nouveau champ d'action dans lequel se déroulent déjà des opérations militaires, la France devra développer une capacité de lutte dans cet espace. Des règles d'engagement appropriées, tenant compte des considérations juridiques liées à ce nouveau milieu, devront être élaborées. » Les États veulent garder une prééminence du national sur le domaine du numérique qui n'est pas perçu comme un territoire comme les autres. Après la terre, la mer et l'espace, le nouveau territoire à intégrer c'est le cyberspace.

Comment cela se traduit-il concrètement sur le terrain ?

Dans cette cyberguerre, on apprend en marchant. La France est ainsi en train de bâtir de manière encore informelle et assez empirique une doctrine de sécurité de l'information sur le champ de bataille. En visite en Afghanistan, le général Elrick Irastorza, chef d'état-major de l'armée de terre, a interdit aux soldats en missions sur les théâtres d'opération d'envoyer des images et des SMS avec leur téléphone portable. Aussi surprenant que cela

puisse paraître, la couverture GSM fonctionne en Afghanistan et on s'est aperçu que les militaires envoyaient des photos à leur famille ou pour nourrir des milblog, avec tous les risques que la divulgation incontrôlée de telles informations sensibles ou stratégiques faisait peser sur les forces engagées. Cette vulnérabilité numérique liée à de nouveaux comportements est désormais prise en compte même s'ils n'avaient pas été anticipés.

La numérisation de l'espace de bataille intègre certes la révolution des nouvelles technologies mais est-elle adaptée aux conflits asymétriques auxquels sont confrontées nos forces, en Afghanistan par exemple ? N'y a-t-il pas là un risque d'aveuglement technologique en total décalage avec la réalité du terrain qui nécessite une certaine rusticité en privilégiant le renseignement humain ?

La numérisation du champ de bataille est une avancée indéniable et pourra fonctionner pour certains espaces de bataille mais il est vain de penser qu'il faille équiper systématiquement la totalité des combattants sur l'ensemble des théâtres d'opérations. Le meilleur rempart contre le tout technologique est avant tout budgétaire lorsque l'on connaît par exemple le coût d'équipement du système FELIN pour un fantassin. La numérisation de l'espace de bataille propose des outils technologiques performants mais la guerre ne sera jamais une partie de jeux vidéo car elle reste une confrontation sanglante d'individus les uns aux autres. La numérisation du champ de bataille ne doit pas transmettre à l'opinion publique l'idée qu'en investissant dans ces technologies on s'épargne toute perte humaine, dans ce mythe d'une guerre virtuelle de zéro mort. Nous sommes plus dans une adjonction avec la cyberguerre par rapport à un théâtre d'opération existant et à une opération militaire plutôt que dans un remplacement.

Quelle révolution stratégique ces nouvelles capacités d'information numérique déclenchent-elles au sein des forces armées ? La dépendance technologique qui en découle ne va-t-elle pas développer de nouvelles vulnérabilités ?



La préoccupation des armées va être de réussir à intercepter, court-circuiter ou fausser les informations émanant de fantassins équipés de systèmes de communication reliés à leur état-major. L'objectif pourra être de neutraliser à distance les forces armées comme la Russie a réussi à clouer au sol l'aviation géorgienne. L'avantage stratégique sera donné à celui qui aura la capacité de contrer les cyberattaques mais également de maintenir sa capacité opérationnelle malgré la perte de tous ses réseaux. L'exemple estonien a montré que plus une société est numérisée et dépendante de ses réseaux et plus les conséquences d'une cyberattaque sont importantes. Cependant le pouvoir estonien a su trouver une solution de remplacement à l'identique pour ses sites gouvernementaux via les sites d'hébergement Blogger de Google. Ce qui démontre que si le numérique développe de nouvelles vulnérabilités face à des cyberattaques, sa capacité de résistance et de résilience est aussi totalement inédite avec des solutions de remplacement à l'identique. Les attaques peuvent avoir des effets dévastateurs inédits mais les réponses et les capacités des réactions qui se développent en réaction sont également totalement inédites.

L'autonomie vis-à-vis des réseaux soulève la question de la gouvernance d'internet et de l'indépendance stratégique de la France en la matière ?



« Nous sommes encore à ce jour en France dans une logique purement défensive : la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI), placée au SGDN, c'est la citadelle qui a vocation à surveiller le net et à repérer les agressions dont les ministères, les administrations et les grands centres stratégiques peuvent faire l'objet en France. »

On peut légitimement se poser la question du contrôle d'internet lorsque l'on sait que le réseau a été créé à l'origine pour doter les militaires américains d'un système de communication qui pourrait résister à une explosion nucléaire. L'ICANN (Internet Corporation for Assigned Names and Numbers) qui gère ce réseau depuis 1998 est une association qui siège en Californie et qui est placée sous l'égide du ministère américain du Commerce. On comprend que l'ICANN qui contrôle les adresses internet a le contrôle total par la même occasion de l'information circulant sur le réseau (sites et courriels).

Comment réagissent les autres puissances ?

Si les Européens semblent se satisfaire de cet état de fait, la Chine, qui compte déjà 300 millions d'internautes, envisage pour son indépendance de se doter d'un réseau de communication 100% chinois constitué notamment de ses propres adresses IP, mais qui resterait interopérable avec le reste de la toile mondiale. Si d'autres pays comme l'Inde adopte la même stratégie, on assisterait alors à un morcellement de l'Internet.

La Russie quant à elle souhaite maîtriser et pouvoir contrôler l'ensemble des informations téléphoniques et internet qui transitent sur son territoire. Le ministère des communications russe oblige les fournisseurs d'accès à internet et les opérateurs de téléphonie présents dans la fédération de Russie et dans plusieurs pays de la CEI à connecter leurs serveurs sur SORM, un système de surveillance directement administré par le service de renseignement du FSB. Contrairement à l'Europe, la Russie a pleinement intégré la dimension de la cyberguerre dans sa politique militaire comme le confirment les épisodes géorgiens et estoniens.

La France développe-t-elle sa propre capacité de contrôle du web ?

La Chine, la Russie et les États-Unis ont pris d'autorité cette position de contrôle des réseaux. L'univers numérique a beau être virtuel, l'autorité politique peut imposer un passage sous les fourches caudines de son instance de défense et de sécurité. Aujourd'hui la France n'est pas en mesure techniquement de la faire et politiquement d'assumer un système de contrôle. L'État a pourtant un rôle hautement stratégique à assumer dans les cyberconflits qui se profilent bien loin des champs de bataille traditionnels, s'il ne souhaite pas voir disparaître des pans majeurs de notre souveraineté et subir une forme d'inféodation numérique.

Comment se prépare-t-on à la cyberguerre ?

Sur le plan de la sécurité, la France a l'habitude d'agir a posteriori en réaction à un événement tragique ou évité. La France a toujours envisagé la sécurité de manière curative. Nous sommes encore à ce jour dans une logique



« Les États veulent garder une prééminence du national sur le domaine du numérique qui n'est pas perçu comme un territoire comme les autres. Après la terre, la mer et l'espace, le nouveau territoire à intégrer c'est le cyberspace. »

défensive de la Direction Centrale de la Sécurité des Systèmes d'Information, placée au SGDN. C'est la citadelle qui a vocation à surveiller le net et à repérer les agressions dont les ministères, les administrations et les grands centres stratégiques peuvent faire l'objet en France. Une future Agence qui aurait le statut d'établissement public à caractère industriel et commercial, à l'instar du CEA, permettrait de regrouper tous les acteurs de cette cyberguerre dont ceux chargés des opérations offensives.

Comment cette agence va-t-elle recruter des cyberguerriers ?

Nous sommes là sur une activité essentiellement humaine où les capacités individuelles sont au cœur des compétences d'un « cyberguerrier ». Mais le cadre naturel pour exercer un métier de cyberguerrier ne sera pas naturellement ou exclusivement cette Agence, contrairement à l'armée qui reste le cadre naturel à des soldats aguerris et formés au combat pour exercer leur métier. La compétence et l'expertise obtenues dans le cadre d'une telle Agence aura une véritable valeur marchande dans le secteur privé. Dans l'univers de la cyberguerre, l'État n'est qu'un employeur parmi d'autres. La grande difficulté sera donc de réussir à attirer les candidats pour intégrer les services de l'État chargés des opérations de cyberguerre et surtout de les garder sans qu'ils partent dans le privé valoriser leur expérience. Par ailleurs, cette Agence aura l'inconvénient d'identifier les personnels chargés de cette cyberguerre, alors qu'il y avait une plus grande discrétion lorsque ce type d'activité était noyé au sein du SGDN. Une discrétion indispensable vis-à-vis des ennemis mais là encore vis-à-vis des chasseurs de tête qui sauront très bien où faire leur marché.

Cette fuite des cerveaux que vous redoutez, ne pourrait-elle pas être justement une manière de propager en dehors du cadre étatique une culture de cyberdéfense et l'occasion de tisser un réseau de correspondants dans le secteur privé ?

Pour cela il faudrait une logique de mémoire et que les candidats ne rentrent pas dans le dispositif de cyberdéfense français avec dès le départ en arrière-pensée la valorisation dans le privé deux ans plus tard. Comme

ceux qui planifient de faire l'École des impôts pour pouvoir très vite intégrer un cabinet fiscal. La future Agence nationale de sécurité des systèmes d'information devra donc mettre en place une véritable gestion des carrières pour les métiers de la cyberguerre. Dans l'univers hyper innovant et bouillonnant des nouvelles technologies de l'information ce n'est pas le plus âgé dans le grade le plus élevé qui a raison. La qualité de la cybersécurité n'aura rien à gagner à un *turn-over* constant des personnels, et j'y vois au contraire un point de faiblesse considérable et un obstacle à la constitution d'un véritable capital informationnel, un capital de mémoire sur les cybercrises passées.

La solution peut-elle passer par une « militarisation » de cette fonction de cyberdéfense ?

Nous sommes là dans une affaire de compétences alors faut-il prendre des techniciens que l'on militarise ou trouver des militaires ayant le bon profil. Les gendarmes ont très bien su le faire pour lutter contre la cybercriminalité, notamment sur les questions de pédopornographie, en développant en leur sein une véritable compétence en la matière.

La guerre numérique est menée en très grande majorité par des civils, n'y a-t-il pas là un champ immense de coopération civilo-militaire ?

On peut imaginer avoir recours à des compétences de civils sensibles à ces enjeux de sécurité et d'indépendance stratégique. Il n'est pas sûr que le lien Armée-Nation, renforcé par le passage de hauts responsables d'entreprises dans structures comme l'IHEDN qui ont vocation à contribuer à l'esprit de défense, soit exploité au mieux dans ce domaine. Aux États-Unis, les BENS (Business Executives for National Security) joue sur un engagement patriotique et moral fort et une mise à disposition très spontanée des civils américains pour assurer la sécurité de leur pays. En France nous en sommes encore à essayer d'intéresser les civils aux questions de sécurité et de défense. C'est pourquoi il est important de ne pas enfermer la cyberguerre dans une logique de techniciens.

Pour répondre aux cyberattaques, comment mieux impliquer l'ensemble de la société dans sa propre sécurité à l'image de la défense passive pendant la guerre ?



La force du numérique, c'est qu'il multiplie les champs de bataille. On peut atteindre les militaires comme on peut atteindre l'ensemble de la société. La cyberguerre pénètre notre vie quotidienne en tant que citoyens, consommateurs, salariés, actionnaires, etc. Il doit donc y avoir dans la culture de sécurité de chacun un volet sur les questions cybernétiques qui le concerne. L'erreur serait d'aborder la sécurité numérique sous un angle purement technologique en décalage avec la vie quotidienne. Comme il devrait y avoir dans les écoles un apprentissage des règles de base de secourisme, la cybersécurité devrait être initiée aux enfants comme faisant partie intégrante de leur sécurité et de la

sécurité collective. En matière de cybersécurité la faille est souvent humaine. Il est inutile de construire une superbe structure de cyberdéfense pour la France s'il suffit pour la contourner d'exploiter les vulnérabilités individuelles.

Le cyberterrorisme est-il une menace crédible ?

Tout d'abord la cybercriminalité peut être une source de revenus pour un mouvement terroriste. On peut trouver une réelle complémentarité entre cybercriminalité et cyberterrorisme. Mener des opérations d'escroquerie sur internet peut être un mode efficace de financement d'activités terroristes, comme peut l'être la contrefaçon. Mais à ce jour, on n'en a pas encore détecté mais il n'y a pas de raison pour que cela ne se produise pas car les profils de compétences sont disponibles dans ces mouvements. Les cyberattaques réunissent toutes les qualités d'aisance, de faible coût d'entrée et de fort impact médiatique et économique pour intéresser des mouvements terroristes.

Le terroriste cherche avant tout à tuer. Le monde virtuel peut-il vraiment se transformer en arme de destruction ?

Mettre à bas le système d'information d'un hôpital, couper l'accès à des systèmes de traitement des eaux, dérégler un système de pilotage de l'espace aérien, sont autant de scénarios qui peuvent provoquer par effet de cascade des morts plus du tout virtuels. Les opérateurs qui gèrent les grands réseaux vitaux comme le transport, la distribution d'eau, de gaz ou d'électricité, utilisent tous des systèmes de supervision et de régulation informatisés (SCADA) qui, s'ils venaient à être



Une cyberattaque contre les systèmes SCADA des opérateurs qui gèrent les grands réseaux d'importance vitale pourrait être catastrophique.

piratés et sabotés, auraient des conséquences humaines potentiellement désastreuses. La menace d'une prise de contrôle à distance d'installations critiques comme une raffinerie, un barrage ou une centrale nucléaire est désormais prise en compte par les États et les opérateurs.

Une cyberattaque peut par ailleurs perturber durablement une société en remettant en cause dans l'esprit des citoyens la fiabilité ou la sûreté de tous les systèmes numériques qui peuplent désormais leur quotidien, tout comme l'attaque du 11 septembre a laissé des séquelles chez certaines personnes qui prennent l'avion ou travaillent dans des tours.

Peut-on quantifier un préjudice numérique et chiffrer le coût de la cybercriminalité ?

Le nombre de victimes potentielles augmente avec la généralisation d'internet dans la société mais les réseaux sociaux comme Myspace ou Facebook, en livrant une somme d'informations personnelles participent à la fragilisation de leur propre cybersécurité et favoriseraient incontestablement les agressions. Les dépôts de plaintes ne sont pas représentatifs car souvent les victimes ne savent pas qu'elles ont été attaquées ou ne souhaitent pas porter plainte pour préserver leur image. Les éditeurs de logiciels de sécurité ou les assureurs livrent des rapports annuels très détaillés et souvent alarmistes sur les menaces informatiques; rapport que l'on ne peut qualifier d'impartialité car ils ne sont bien évidemment pas dépourvus d'une certaine démarche commerciale. Mais à l'instar des assureurs, il doit y avoir adéquation entre le coût du mode de protection et la valeur du bien à protéger. Pour cela il faut être capable de jauger la valeur d'une information à protéger. Mais comment évaluer l'immatériel face à un ennemi invisible, c'est le défi qu'il reste à relever dans notre société de l'information.

Propos recueillis par Christophe Boucher