diploweb.com La revue géopolitique
ISSN : 2111-4307

Dossier géopolitique. Le cyberespace : conflictualité et coopération

dimanche 13 avril 2025,par Pierre VERLUISE

Citer cet article / To cite this version :
Pierre VERLUISE, **Dossier géopolitique. Le cyberespace : conflictualité et coopération** , *Diploweb.com : la revue géopolitique, 13 avril 2025.*

L’actualité impose plus que jamais le cyber au nombre des préoccupations. Attaques, ingérences, dépendances… et quête d’autonomie sont à mettre en perspective. C’est ce que vous propose ce dossier. Etudes, entretiens, articles, cartes, vidéos… Voici plusieurs dizaines de documents d’experts qui se font pédagogues. En effet, le Diploweb attire l’attention depuis plus d’une décennie sur la dimension géopolitique et stratégique du cyber. En voici les preuves. Ce dossier dirigé par Pierre Verluise est aussi un clin d’oeil amical aux enseignants d’HGGSP de Terminale qui ont a enseigner : Le cyberespace, entre réseaux et territoires (infrastructures, acteurs, liberté ou contrôle des données…) ; Cyberdéfense, entre coopération européenne et souveraineté nationale : le cas français.

. Florian Manet, Pierre Verluise, Emilie Bourgoin, La géopolitique résiste-t-elle au cyber ?

Le cyber, est-ce virtuel, immatériel ou matériel ? De quelles façons la couche matérielle du cyber est-elle un champ d’affrontement géopolitique entre acteurs étatiques mais aussi non étatiques ? Pourquoi la couche logicielle du cyber est-elle l’enjeu de l’expression des rivalités de puissance étatique comme non étatique ? Comment pouvons-nous comprendre la géopolitique des infrastructures numériques ? Dans le cyber, l’État est-il un acteur disqualifié ? Pour répondre, nous avons l’honneur de recevoir Florian Manet. Podcast et synthèse rédigée validée par F. Manet.

. Kévin Limonier, Pierre Verluise, Jérémie Rocques, Vidéo. Géopolitique du cyber. Comment circulent les données ?

Cette vidéo est un extrait gratuit de "Pourquoi les données numériques sont-elles géopolitiques ?" Masterclass de Kévin Limonier. Voici la session Comment circulent les données ?

. Arnaud Coustillière, UE. Quel chemin pour conquérir notre autonomie stratégique numérique ? Trump un électrochoc salutaire !

La route sera longue, mais l’électrochoc de la prise de pouvoir par le président Trump et de son écosystème a le mérite de nous montrer que le monde d’avant est terminé ; que celui de demain parait surtout marqué par l’incertitude, les rapports de force et les volontés de domination.

L’Europe est seule et doit reprendre en main son destin. Cela passe aussi et de façon très importante par la défense militaire, la puissance économique et le numérique qui irrigue aujourd’hui tous les pans de nos sociétés.

. Kévin Limonier, Pierre Verluise, Jérémie Rocques, Vidéo. Cartographier les données numériques pour mieux comprendre les rivalités

Cette vidéo est un extrait gratuit de "Pourquoi les données numériques sont-elles géopolitiques ?" Masterclass de Kévin Limonier. Voici la session Cartographier les données pour mieux comprendre les rivalités, un défi méthodologique.

Pierre Verluise
Docteur en géopolitique, fondateur du *Diploweb.com*
Verluise

. Anastasia Kryvetska, Comment l'écosystème cyber ukrainien s'est-il adapté à la guerre ?

Depuis 2014, le moteur du développement du cyberespace ukrainien est la guerre avec la Russie. Même si les autorités ne sont pas parvenues à agir efficacement dans le cyberespace dès le début du conflit, ce dernier a fait émerger un écosystème cyber qui a su s'adapter au contexte de guerre. Cet écosystème a contribué à la défense du pays à toutes les échelles, tant au niveau des citoyens que des acteurs étatiques et privés. Bien que de très nombreux objectifs doivent encore être atteints, l'invasion de l'Ukraine est un catalyseur pour le développement du cyber, qui est devenu un acteur essentiel du ministère de la Défense. Illustré de trois graphes.

. Pascal Martin, L'action cyberoffensive comme nouvelle capacité au profit d'une diplomatie coercitive

La diversité des opérations pouvant être menées dans le cadre de la cyber-conflictualité permet de conduire une forme de guérilla quotidienne qui ne cherche pas à détruire son adversaire mais dans laquelle les défenseurs s'épuisent à tenter de parer chaque coup. Cette forme de lutte est également utilisée et mise en œuvre par certains États, dans le cadre d'une stratégie indirecte. Dès lors, les actions cyberoffensives peuvent utilement servir à une doctrine de diplomatie coercitive.

Cet article s'attache à exposer la dualité d'emploi de l'action cyberoffensive dans les relations interétatiques : une nouvelle capacité offensive au profit d'une diplomatie coercitive, conduisant à un engagement de nombreux acteurs dont les services de renseignement, et une approche défensive reposant sur la décision politique d'attribution des cyberattaques.

. David Colon, Pierre Verluise, La guerre de l'information cherche à accélérer la décomposition des sociétés démocratiques

Comment définir la guerre de l'information ? Comment les adversaires des Etats-Unis, notamment l'Iran, la Chine, la Russie ont-ils réagi à la guerre de l'information conduite par les Etats-Unis ? Quelles sont les fonctions des agences de presse et des médias sociaux dans la guerre de l'information contemporaine ? Que font les Etats-Unis mais aussi les États membres de l'UE pour se prémunir de la guerre de l'information conduite par la Russie mais aussi la

Chine ?

Voici un entretien majeur avec l'auteur d'un des meilleurs ouvrages publiés depuis trente ans sur la désinformation, enjeu majeur des temps présents et futurs. Vous allez connaitre les grands moments et les principaux acteurs d'une guerre à laquelle nous n'étions pas préparés, devenue menace mortelle pour nos démocraties.

David Colon, auteur de « La guerre de l'information. Les États à la conquête de nos esprits », Ed. Tallandier, répond aux questions de Pierre Verluise pour Diploweb.com. Avec en bonus la vidéo d'une conférence de D. Colon accompagnée de sa synthèse validée.

. Pascal Martin, Les services de renseignement comme acteurs de la coercition cyber à des fins géopolitiques

Le cyberespace offre un nouveau champ d'expression pour l'action clandestine. En effet, le cyberespace a permis l'apparition d'"illégaux virtuels". Un parallèle peut être fait entre les moyens de cyberattaque persistante et les agents clandestins si l'on considère les modes opératoires, le soutien logistique, la nature des missions et les objectifs géopolitiques.

La révolution numérique a de larges impacts sur les modes opératoires offensifs possibles car elle est le corollaire d'une innovation continue où l'interconnexion générale des différents secteurs de l'économie et de la société accroît les vulnérabilités. Cette numérisation croissante des sociétés et des individus a donc rapidement été initiatrice de nouveaux comportements transgressifs, mais également de nouveaux modes opératoires permettant à des structures étatiques, ou des groupes « para-étatiques » soutenus et tolérés par l'État officiellement ou clandestinement, de contraindre des adversaires sans revendication officielle de l'attaquant.

. Pascal Martin, L'attribution publique des cyberattaques comme stratégie diplomatique défensive

Les actions cyberoffensives, info-centrées et variées dans leur nature, peuvent être exploitées au profit d'une diplomatie coercitive selon deux approches distinctes, mais complémentaires : offensivement, à travers des opérations cyberclandestines mises en œuvre par les services de renseignement, leurs proxies ou des structures vassalisées mais démarquées ; ou défensivement, en procédant à l'attribution officielle d'une action cyberoffensive selon les enjeux politiques, conjoncturels ou non, en s'appuyant sur l'analyse techno-centrée réalisée avec l'appui des services de renseignement.

. Anastasia Kryvetska, Renseignement, cyberguerre et nouvelles technologies : les civils sont-ils un moyen asymétrique redoutable dans la guerre en Ukraine ?

La guerre russe en Ukraine a été à l'origine de la "première cyber-guerre mondiale". Anastasia Kryvetska présente de manière documentée l'indispensable rôle de l'« arrière » dans ce conflit au cœur d'une reconfiguration du monde. Nul doute que de nombreux états-majors se penchent sur ces évolutions à la fois techniques et sociétales… quand les pays de l'UE se trouvent sommés de compenser les aléas américains.

. Marie-Gabrielle Bertran, La recherche d'une souveraineté numérique en Russie : à qui profite-t-elle ?

Les liens entre le secteur privé et les institutions publiques dans le domaine du numérique en Russie sont le témoignage des nouvelles logiques de cyberdéfense du pays. En effet, ils concourent à la construction d'une souveraineté numérique russe, en partie destinée à protéger ses réseaux. Mais ils sont aussi le signe de l'influence majeure de certains acteurs privés sur les autorités, via, notamment, un rôle de conseil décisif dans l'établissement des nouvelles législations et doctrines sur le numérique en Russie.

. Aline Amodru-Dervillez, Quelles sont les chances de la France dans la bataille numérique en Océanie ?

Dans un environnement géopolitique mouvant, les collectivités françaises du Pacifique développent une stratégie pour devenir des acteurs majeurs de l'Océanie et créer un « Pacific French Tech ». Les enjeux sont considérables, et les difficultés restent présentes. Cette étude solidement documentée est à la fois un éclairage des collectivités françaises d'outre-mer en Océanie, et une présentation d'une dimension méconnue des enjeux numériques présents et à venir. Quatre cartes inédites.

. Jonathan Guiffard, Quelles représentations ont amené le gouvernement américain à choisir une stratégie de soutien indirect de l'Ukraine basée sur le cyber et le renseignement ?

La confrontation de représentations variées et divergentes ont mis le gouvernement américain sous une forte tension, l'amenant dès 2014 à mener une politique de soutien indirect aux Ukrainiens, politique qui a changé d'ampleur mais pas de nature en février 2022. Cette absence de changement résulte de l'équilibre de ce conflit de représentations qui n'a pas sensiblement évolué avec l'invasion russe de grande ampleur. Dans cette logique indirecte, le partage de renseignement et l'appui en cyber ont constitué des dimensions privilégiées, permettant d'obtenir des résultats importants pour la sécurité ukrainienne mais aussi américaine.
Avec une carte sur "Les représentations américaines d'une menace russe stratégique" et une "Frise de l'évolution des représentations américaines à l'égard de la Russie".

. Sébastien Baptiste, La cyberdéfense militaire française à l'épreuve des Jeux Olympiques et Paralympiques de 2024

Le cyberespace est le théâtre d'une guerre permanente. C'est aussi le support principal des échanges sociaux et économiques, faisant de chaque cyberattaque un facteur de déstabilisation du quotidien. Les Etats et les groupes organisés qui y ont recours font preuve de toujours plus d'audace, frappant avec une apparente impunité. La défense semble désavantagée du fait de son coût d'installation et de mise en œuvre mais surtout, elle n'a pas l'initiative. Un adversaire n'a besoin que d'une faille et choisit quand il l'exploite. Le défenseur doit surveiller l'entièreté de son périmètre, et ce constamment. Les systèmes militaires ne sont pas épargnés, et font quotidiennement objets d'actions malveillantes. A l'approche des Jeux Olympiques et Paralympique de 2024 (JOP 2024), cet article vise à identifier les enjeux de la cyberdéfense militaire dans la préparation aux menaces de demain.

. Laura Brincourt, Le "Cloud Act", trois ans après : révélateur du besoin de définition de notre souveraineté dans l'espace numérique

Au coeur des facteurs enchevêtrés du numérique, se joue une partie essentielle de notre souveraineté. Le Cloud Act des Etats-Unis n'est qu'un révélateur d'un besoin plus général : la définition d'une véritable stratégie nationale et européenne dans l'espace numérique ciblée sur des secteurs et des technologies phares. Il nous faut redevenir stratèges dans une époque dominée par la donnée où chacun a son rôle à jouer pour gagner en souveraineté. Cet article s'intéresse aux besoins, pour l'Etat et les entreprises, de s'organiser, de s'adapter mais aussi de collaborer avec les puissances du numérique dans une géopolitique inédite des données.

. Alix Desforges, Vidéo. Méthode et des concepts de l'analyse géopolitique pour analyser les enjeux liés au cyber espace

En ouverture d'une conférence de B. Loyer, Alix Desforges, post-doctorante au sein du centre de recherche et de formation "Géopolitique de la datasphère" (GEODE) à l'Institut Français de Géopolitique (Université Paris 8) propose un questionnement centré autour de la pertinence de la méthode et des concepts de l'analyse géopolitique pour analyser les enjeux liés au cyber espace, par . Le cyber espace est une question relativement récente et qui semble profondément technique, pourtant elle est avant tout une question hautement géopolitique. Loin de n'être qu'un espace virtuel, le cyber espace cristallise des conflits et des rivalités entre de multiples acteurs et est le vecteur d'attaques géopolitiques, pour devenir lui-même un véritable théâtre d'opérations militaires. La démonstration s'appuie sur le triptyque de la méthode géopolitique.

. Bruno Dupré, Espaces communs : espaces contestés et stratégiques

Qu'il s'agisse des océans, du cyber, de l'espace extra-atmosphérique ou encore de l'Arctique, les espaces communs - appelés comme tels car ils sont au-delà des juridictions nationales – sont aussi des espaces contestés faisant l'objet d'enjeux de gouvernance internationale, mais aussi et surtout de souveraineté avec une tension grandissante entre grandes puissances. L'Union européenne a commencé à se positionner mais doit s'adapter en permanence pour défendre ses propres intérêts et valeurs.

. Laurent Bloch, Hégémonie juridique dans le cyberespace

L'industrie informatique et l'Internet sont des créations américaines et les Européens ont la plupart du temps été des suiveurs, malgré quelques exceptions brillantes. Il n'est donc pas surprenant que les représentants d'institutions et de compagnies américaines occupent des positions clé dans les organismes de normalisation et de pilotage des domaines techniques et organisationnels de ces industries.

. Florian Manet, Thalassopolitique des fonds marins, théâtre d'une nouvelle conflictualité inter-étatique ?

Matérialisée par le conflit russo-ukrainien et ré-affirmée au Proche-Orient depuis l'attaque par le Hamas d'Israël, la nouvelle donne stratégique a des incidences directes et immédiates sur les politiques de défense des États, contraints d'adapter la protection de leurs intérêts majeurs. La maritimisation des modes de vie conjuguées à la digitalisation des économies et aux objectifs de transition énergétique ont dessiné, notamment, une géopolitique énergétique et numérique qui est questionnée aujourd'hui. En effet, ces dynamiques reposent sur des réalisations industrielles à l'image des câbles sous-marins (énergie, télécommunication), des

plates-formes d'extraction de matières premières (hydrocarbures, terres rares…) mais aussi les projets d'envergure des îles énergétiques artificielles. Ces infrastructures critiques sous-marines et maritimes sont devenues des centres de gravité stratégiques qui conditionnent la résilience des États. Transparentes pour l'usager, elles constituent, néanmoins, selon les points de vue, soit des vulnérabilités soit des cibles d'intérêt dans la perspective d'une guerre totale ou guerre d'attrition. Florian Manet se fait pédagogue pour expliquer les ressorts de ces nouveaux risques majeurs et met les États devant leurs responsabilités.

. Charlotte Bezamat-Mantes, ECFR, Carte. Les principales cyber-puissances

L'ECFR a publié en anglais une somme considérable "The Power Atlas. Seven battlegrounds of a networked world", sur ecfr.eu. Un membre du Conseil scientifique du Diploweb a attiré notre attention sur cette publication. Nous avons demandé à l'ECFR l'autorisation de traduire quelques cartes en français afin de contribuer au débat. Traduite et réalisée en français par C. Bezamat-Mantes, la carte grand format est accompagnée d'un court commentaire.

. Grégory Joubert, Existe-t-il un cyberespace centrasiatique ?

L'annonce de la mise en retrait relatif du président Noursoultan Nazarbaïev, le 19 mars 2019, a attiré l'attention sur le Kazakhstan, ex-république soviétique d'Asie centrale de 2,7 millions de km2 (18,4 millions d'habitants). L'occasion de se poser une question : existe-t-il un cyberespace centrasiatique ? La première partie de cette étude solidement documentée a pour principal objectif de traiter de la dépendance infrastructurelle des États d'Asie centrale à la Russie. Sur la base de ces considérations, une deuxième partie présente le vecteur d'influence que constitue le cyberespace, ainsi que de la perception que se fait le pouvoir kazakhstanais de ce terrain conceptuel. De l'influence informationnelle subie à l'absence de prise en compte de l'aspect profondément technique du cyberespace, le Kazakhstan est foncièrement un État vulnérable. Dans la troisième partie, Grégory Joubert se penche plus particulièrement sur les leviers d'action utilisés par les autorités pour le contrôle des activités de la population en ligne et les moyens de surveillance dont dispose le pays. Outre son intérêt propre, cette étude peut aussi être féconde pour réfléchir aux relations entre les pays de l'Union européenne et une autre puissance de l'Internet, les Etats-Unis.

. Arsenio Cuenca, La France face à la géopolitique de la 5G : quels enjeux autour de la nouvelle génération de réseau sans fil ?

Quels sont les enjeux liés au déploiement de la technologie 5G au niveau européen et plus précisément, dans le cas de la France ? Une réponse solidement documentée et finement argumentée. Arsenio Cuenca précise d'abord les enjeux éminemment géopolitiques autour de cette technologie innovante. Puis il présente la réaction européenne face à sa situation de dépendance. Enfin, l'auteur brosse l'évolution des représentations autour du système d'alliances français et les agendas public-privés pour un avenir numérique.
Illustré d'une carte sur le problème de la dépendance technologique en Europe et d'une perspective diachronique des enjeux de la 5G en France.

. Isabelle Tisserand, Antonin Dacos, Cyberdéfense de l'Espace : un nouveau défi international

Quel est l'intérêt stratégique des satellites aujourd'hui ? Peut-on parler de prolifération et de

compétition aujourd'hui ? En quoi la question de la protection informatique des satellites est-elle cruciale ? Quelles sont nos capacités de résilience face aux attaques contre des satellites ? Voici quelques-unes des questions auxquelles répond I. Tisserand. Propos recueillis par A. Dacos pour Diploweb.com.

. L'OTAN dans la cyberguerre : stratégie globale et capacités opérationnelles

Quelles sont les problématiques de la cyberdéfense de l'OTAN ? L'auteur présente un tableau d'ensemble très utile pour saisir l'ampleur des défis de ce champ opérationnel particulier.

. Frédérick Douzet, Chine : cyberstratégie, l'art de la guerre revisité

La Chine est devenue un acteur majeur et incontournable du cyberespace, avec une volonté claire d'exister, de développer ses outils stratégiques et de ne pas dépendre technologiquement d'autres nations pour maîtriser au mieux l'information stratégique. Bien que le régime ait développé d'importantes cybercapacités, elles semblent moins centralisées, coordonnées et maîtrisées que ce que les discours sur la menace chinoise laissent à croire. Dans le brouillard juridico-stratégique du cyberespace, la Chine pousse cependant son avantage en menant des offensives de basse intensité et une politique de renseignement et d'influence qui témoigne de sa volonté de fomenter les outils de sa puissance et de se positionner comme un acteur avec lequel il faudra compter.

. Estelle Hoorickx, Les menaces hybrides : quels enjeux pour nos démocraties ?

Les menaces hybrides : de quoi parle-t-on ? Quels sont les outils hybrides de plus en plus nombreux et diversifiés qui nous menacent ? Quels sont les principaux acteurs des attaques hybrides ? Estelle Hoorickx fait œuvre utile en précisant les concepts, les stratégies et les moyens utilisés pour nuire aux démocraties en les polarisant à outrance. Les défis sont considérables. Seul un effort durable et conjugué de l'UE et des autres démocraties, impliquant l'ensemble des sociétés civiles, peut produire des effets bénéfiques sur le long terme.

. Pierre Buhler, La puissance : quelles métamorphoses ?

Au cours de ces 25 dernières années, la redistribution de la puissance s'est opérée à un rythme inédit. La révolution numérique a conduit à un ébranlement des États, tandis qu'un phénomène classique de "transition de puissance" produit un déplacement l'Occident vers l'Asie du centre de gravité du monde. Ces métamorphoses de la puissance n'en sont qu'à leurs prémices.

. Kevin Limonier, Internet en URSS : à la barbe du régime

L'auteur retrace le développement – en apparence paradoxal – d'un réseau informatique libre et ouvert en Union Soviétique à compter des années 1980. Cette étude lève un voile sur l'histoire de l'Internet comme sur celle de l'URSS.

. Olivier Kempf, Stratégie du cyberespace

Une rupture stratégique, l'avènement du cyberespace ? Oui, répond Olivier Kempf, parce que le cyber est opaque et non létal. L'offensive redevient possible, avec un allongement du temps

stratégique, contrairement à une idée répandue. Et une question : une guerre cyber peut-elle déborder en guerre classique ?

. Laurent Bloch, Surveillance américaine sur l'Internet. Antécédents et conséquences

Les dispositifs d'espionnage de la NSA ne datent pas d'hier. Par ailleurs, même si c'est avec moins de moyens, les autres pays en font autant. Qu'y a-t-il donc de nouveau avec les révélations de l'affaire Snowden ?

. François-Bernard Huyghe, Olivier Kempf, Yann Derriennic, Maxime Arquillière, Gagner les cyberconflits, au-delà du technique

Cet entretien exclusif fait un vaste tour d'horizon des problématiques stratégiques et géopolitiques des cyberconflits. Afin d'offrir à chacun les clés de lecture des nouveaux enjeux. Avec le cyber, le monde a changé, encore faut-il disposer des éléments nécessaires pour en prendre la mesure. Les voici.

. Yannick Harrel, Le concept américain de nouvelle frontière : de la conquête de l'Ouest au cyberespace

La conquête de l'Ouest, la Lune, le cyberespace : voilà trois figures de la frontière pour les Etats-Unis. Autant de facteurs de puissance, une puissance réinventée du XVIIIe siècle à nos jours. Y. Harrel éclaire avec une grande maitrise deux siècles et demi d'histoire. Il démontre la fonction géopolitique de la frontière pour les Etats-Unis dans leur réinvention permanente de la puissance.

. Kevin Limonier, Laurent Bloch, Pierre Verluise, Fabien Herbert, Vidéo. La bataille de l'Internet : Etats-Unis / Russie, un point partout ?
Laurent Bloch et Kevin Limonier, experts d'Internet, répondent en vidéo aux questions du Diploweb.com (8 minutes). Clair et pédagogique. Très utile pour comprendre cette nouvelle dimension de la conquête de la puissance.

. Nicolas Mazzucchi, Pierre Verluise, Fabien Herbert, Estelle Ménard, Vidéo. La cyberconflictualité dans le monde, analyse géopolitique et stratégique

Voici les clés pour comprendre la cyberconflictualité, une réalité importante du monde d'aujourd'hui, et plus encore de demain. Chargé de recherche à la Fondation pour la recherche stratégique (FRS), Nicolas Mazzucchi répond aux questions de Pierre Verluise, Fondateur du Diploweb.com (7 minutes)

. Laurent Bloch, Un nouvel espace stratégique, le cyberespace

Laurent Bloch explique le principe des espaces publics, le modèle en couche du cyberespace, et les facteurs de puissance dans le cyberespace. Ce chapitre est extrait d'un ouvrage de Laurent Bloch, "L'Internet, vecteur de puissance des Etats-Unis ?" publié par Diploweb. Ce livre est disponible sur Amazon au format numérique Kindle et au format broché imprimé sur papier.

. Thierry Berthier, Internet. Géopolitique de la donnée. Maîtriser la donnée : enjeux et

[défis géopolitiques. Moteurs de recherche et web profond]

Pourquoi la donnée peut-elle être considérée comme une ressource qui, une fois exploitée, créé de la valeur et de la puissance ? L'auteur répond clairement en présentant successivement comment les moteurs de recherche sont des vecteurs de puissance, mais aussi les défis du web profond et la dépendance excessive de l'Union européenne.

. Laurent Bloch, Hégémonie des États-Unis sur l'Internet

Laurent Bloch présente ce qu'est l'Internet, le contrôle des normes et de la gouvernance, la domination des infrastructures et des industries américaines.
Diploweb.com, publie dès 2015 cet ouvrage de Laurent Bloch, "L'Internet, vecteur de puissance des Etats-Unis ?" pour proposer à chacun les éléments nécessaires à une juste appréciation de la situation. Ce livre est disponible sur Amazon au format numérique Kindle et au format broché imprimé sur papier.

. Cassini, Florian Carrelet, Cartes. Vers un Internet russe ?

La géopolitique de l'Internet est un axe majeur de la transformation du monde. Voici trois cartes inédites pour présenter "La Russie et la crainte d'un Internet sous domination occidentale" ; "Moscou et la Sibérie, centres d'un Internet russe en mutation" ; "L'Internet russe : l'émergence d'une puissance régionale".

. Laurent Bloch, Internet : que faire pour défendre nos chances ?

En matière d'Internet, quels sont les atouts de la France ? Et de l'Union européenne ? Les atouts de la France et de l'Union européenne sont-ils valorisés pour optimiser leurs poids relatifs, si oui comment, sinon pourquoi ? Pour l'heure, quels sont les gagnants de cette situation ? À l'échelle de la France, que faudrait-il faire d'ici 2030 ? À l'échelle de l'UE ?

. Marie-Christine Dupuis-Danon, Alain Bauer, Pierre Verluise, Comment le renseignement français change-t-il ?

Comment définir « le renseignement à la française » ? Comment s'est-il adapté aux grandes ruptures stratégiques ? Quelles relations entre services de renseignement, responsables politiques et médias ? Les pays « alliés » s'espionnent-ils ? Quelles sont les opportunités et les défis du temps présent ? La dernière question de l'entretien concerne le cyber et l'intelligence artificielle.

. Charlotte Bezamat-Mantes, Laurent Bloch, Pierre Verluise, Carte de l'Internet : quelle hiérarchie des puissances ?
Cette carte de l'Internet présente des acteurs inégaux… et de remarquables moyens de renseignement. Concernant les acteurs, la carte distingue les cyberpuissances, les 4 cyber-dragons, les déserteurs du cyber-espace, un acteur secondaire et un quasi-absent. Les moyens de renseignements sont les câbles sous-marins, les points d'accès de la NSA aux stations d'atterrissage des câbles, et un modèle de sous-marin américain capable de faire des branchements secrets sur des câbles immergés.

Toujours plus sur Diploweb

Ce dossier présente une sélection non exhaustive des ressources du Diploweb disponibles sur le cyber. Plusieurs dizaines de documents s'y rapportent. Aussi nous vous invitons à poursuivre et affiner votre exploration de deux façons :
. par l'utilisation du moteur de recherche interne (en haut à gauche) ;
. par l'usage des rubriques géographiques du menu, en fonction de votre zone d'intérêt.

P.-S.

Docteur en géopolitique de l'Université de Paris IV – Sorbonne, Pierre Verluise est fondateur du premier site géopolitique francophone, *Diploweb.com*. Il en est le directeur des publications. Producteur géopolitique (articles, études, émissions de radio, livres, conférences, concours, formations, vidéos, etc.). Auteur ou co-auteur ou directeur d'une trentaine d'ouvrages sur la géopolitique de l'Europe et la géopolitique mondiale. Auteur de la Masterclass géopolitique "Quels sont les fondamentaux de la puissance ?" disponible sur Udemy. Chercheur associé à la Fondation pour la recherche stratégique (FRS).