DÉCOUVERTE DE LA VIE PUBLIQUE

2e édition

Relations internationales

Xavier Pacreau
Manon-Nour Tannous

En +de 130 Questions réponses

La Documentation française

Sommaire

acteurs transnationaux, de la fragmentation du monde et de la difficulté à construire des alliances.

13 Comment le système international est-il aujourd'hui structuré ?

▶ Aujourd'hui, le système international semble **plus complexe** et moins lisible qu'il ne l'a été pendant la Guerre froide ou dans les années 1990. Bertrand Badie parle de système « post-bipolaire », prenant acte de ce que ce système n'est plus. Il n'est plus non plus unipolaire, les États-Unis étant devenus objet de contestation plus que d'attraction, comme on a pu l'observer dans le champ économique face à la progression de la Chine, ou dans le domaine politique, où ils n'ont pu faire prévaloir leur position face à la Russie lors de la crise syrienne (depuis 2011), ni empêcher la guerre menée par Moscou contre l'Ukraine depuis 2022.

▶ Il s'agit alors de caractériser ce système. Pour certains, le **monde contemporain serait à nouveau bipolaire**, avec la Chine et les États-Unis (si l'on met l'accent principalement sur l'aspect économique des relations internationales) ; ou avec les États-Unis et la Russie, dans ce que certains décrivent comme une nouvelle Guerre froide. L'usage du droit de veto au Conseil de sécurité des Nations unies lors du vote de résolutions concernant les intérêts stratégiques de l'un ou de l'autre, confirmerait cette hypothèse. Mais les tensions entre ces pays ne structurent pas suffisamment la scène internationale pour que l'on puisse se satisfaire pleinement de ce modèle bipolaire.

▶ D'autres propositions théoriques esquissent les contours d'un monde **multipolaire**. Ce modèle permet de prendre en compte la volonté de reconnaissance des pays émergents, et notamment des Brics (Brésil, Russie, Inde, Chine et Afrique du Sud, un groupe élargi le 1er janvier 2024 à quatre autres pays – l'Égypte, les Émirats arabes unis, l'Éthiopie et l'Iran – au sein du « Brics+ »). Un autre terme, celui d'« oligopolarité », désigne un nombre limité de « pôles » (entre cinq et

dix), aucun n'étant assez puissant pour l'emporter contre la coalition des autres, d'où la nécessité de politiques de coopération.

▶ Enfin, une troisième hypothèse se dégage : celle de l'absence de pôle structurant, autrement dit d'un monde **apolaire** voire zéropolaire. Cette proposition découle du constat du manque d'attractivité qu'exercent les grandes puissances, incapables de fédérer autour d'elles. Dès lors, il s'agit de prendre en compte la diversité des acteurs, mais aussi peut-être de cesser de penser en nombre de « pôles ».

Depuis son retour au pouvoir en janvier 2025, la politique du président américain, Donald Trump, laisse quant à elle présager la fin du *leadership* des États-Unis pour les pays occidentaux (notamment l'Europe), un retour au jeu des puissances et la **remise en cause du système international** tel qu'il a été mis en place en 1945.

Un « monde multipolaire »

« La France de Jacques Chirac avait, dans les années 1990, appelé de ses vœux l'émergence d'un monde multipolaire, **mot d'ordre qui n'avait d'ailleurs pas rallié grand monde**, la plupart des pays, Chine et Russie comprises, hésitant à s'associer à cette dénonciation oblique de l'excès de puissance des États-Unis.

En cette décennie 2020, nous y sommes : en 2000, les États-Unis représentaient 20 % du PNB mondial et la Chine, 7 % ; en 2022, c'est respectivement 15 % et 18 %. Ensemble, les économies développées représentaient 57 % du PNB mondial en 2000, et les économies émergentes et en développement 42 % ; ces proportions sont aujourd'hui exactement inverses. La pluralité des pôles de puissance et, parmi eux, des deux principaux, les États-Unis et la Chine, est un fait ».

Source : Gilles Andréani, « Le système international en question », *Questions internationales*, n° 122, décembre 2023-janvier 2024, p. 4-15 (extraits).

États ; de même, des groupes terroristes peuvent déstabiliser certains d'entre eux.

18 Quels sont les éléments de la puissance des États ?

▶ À côté du droit, la **puissance** constitue l'autre facteur de régulation des relations internationales. La puissance d'un État peut s'évaluer par rapport au niveau de liberté d'action dont il dispose ; elle correspond à sa capacité aussi bien à contraindre qu'à influencer les comportements des autres acteurs, donc à orienter le cours des relations internationales.

Il existe des grandes puissances (ou superpuissances) et des puissances régionales. La situation d'« hyperpuissance » (terme utilisé pour la première fois en 1998 par l'ancien ministre des Affaires étrangères Hubert Védrine) peut apparaître lorsqu'une grande puissance n'a plus de concurrent.

▶ Sur le plan militaire, les **puissances nucléaires** correspondent aux États dotés de l'arme atomique (on en compte neuf au 1er janvier 2025 : la Chine, les États-Unis, la France, le Royaume-Uni, la Russie, l'Inde, le Pakistan, Israël et la Corée du Nord). Outre la puissance militaire, l'**assise territoriale**, la **population**, la **géographie** et les **ressources naturelles** constituent des déterminants classiques de la puissance des États. Mais, avec le temps, la notion de puissance a eu tendance à s'élargir à l'économie, la conquête de l'espace, l'industrie, la finance, la culture, l'éducation et aux nouvelles technologies.

Aujourd'hui, la **maîtrise de l'information et des réseaux** qu'elle emprunte tout comme celle de l'**intelligence artificielle** deviennent des composantes essentielles de la puissance des États, tant pour influencer les divers acteurs que pour légitimer leur action. Ces objectifs peuvent aussi concerner les ONG, les firmes transnationales, les OI (organisations internationales) et la société civile.

▶ Facteur de hiérarchisation entre les États, la puissance demeure nécessairement **relative et évolutive**. Elle est en effet tributaire de la combinaison d'un certain nombre de circonstances factuelles et de la situation des autres États.

19 Qu'est-ce que le *soft power* ?

▶ Le *soft power* correspond au **pouvoir d'influence** d'un État ou de tout autre acteur des relations internationales (OI, ONG, firmes transnationales…) **par tous moyens autres que coercitifs** (menace ou emploi de la force), qui relèvent pour leur part du *hard power*, ou « pouvoir de contrainte ». L'importance du *soft power* d'un État est proportionnelle aux moyens de persuasion dont il dispose dans le domaine concerné. Le *soft power* s'exerce autant à l'égard des adversaires que des alliés et vise désormais tous les acteurs des relations internationales.

▶ La **diplomatie**, les **alliances**, la **coopération** institutionnelle (OI) ou non, l'**aide économique**, l'attractivité de la **culture**, la diffusion de l'**éducation** ou le rayonnement d'un **modèle politico-économique** (économie de marché et démocratie par exemple) et de **valeurs** constituent les principaux vecteurs du *soft power*. Il s'agit là d'autant de moyens pacifiques pour convaincre les autres acteurs des relations internationales d'agir ou de se positionner dans un sens donné.

▶ L'efficacité du *soft power* d'un État est également proportionnelle à sa puissance. Mais l'**image** véhiculée par l'État, le **niveau de développement de ses réseaux**, son **histoire** ou l'**autorité de ses dirigeants** peuvent également renforcer l'effectivité du *soft power* qu'il exerce. Il convient enfin de souligner que la garantie de sécurité qu'il représente peut aussi influer sur cette capacité de persuasion. La notion de *smart power* est ainsi parfois employée pour évoquer les effets d'une combinaison utile entre *soft power* et *hard power*.

– d'une faille dans un système d'exploitation ou une application ;
– d'un virus ou d'un cheval de Troie (*trojan horse* ou fonctionnalité maligne dissimulée au sein d'un logiciel légitime) ;
– et, plus généralement, d'un *malware* (logiciel – *software* – malveillant) inséré frauduleusement dans un système informatique, et permettant aux cybercriminels d'accéder à l'ensemble des données qu'il contient.

▶ La cybermenace peut, à l'extrême, concerner la **destruction** potentielle de postes de travail et de systèmes informatiques. Le risque lié à ce type d'attaques tient à la propagation exponentielle de leurs effets délétères en cas d'inaction, ou simplement de défaut de veille appropriée en matière de sécurité informatique. La très grande difficulté d'identification de l'origine exacte de la cybermenace rend son traitement particulièrement malaisé.

La cybersécurité

Le développement très rapide des technologies de l'information et de la communication (TIC) a conduit à une **extension du domaine de la conflictualité dans l'espace numérique** qui concerne désormais non seulement les États, mais également des acteurs publics (ex. : services de l'État, entreprises publiques) et privés, ainsi que des individus ou des groupes d'individus plus ou moins structurés. Le pouvoir égalisateur des nouveaux moyens décentralisés d'agression a donc conduit au développement de techniques de cybersécurité, qui revêtent de multiples aspects. Le cyberespace constitue un nouveau lieu d'interaction et de confrontation, dans lequel les modèles traditionnels en matière de sécurité et de défense ne sont plus véritablement opérationnels.

Dans ce nouvel environnement, où l'origine des menaces d'agression est particulièrement difficile à déceler, la **prévention** prend ainsi une place centrale, au point de constituer désormais un enjeu de souveraineté pour les États. Néanmoins, une capacité offensive cyber permettant de répondre à différents types de cyberattaques constitue également un moyen de dissuasion nécessaire.

Typologie de la menace à laquelle répond la cybersécurité

La cybersécurité se déploie face à **diverses menaces**, qui peuvent avoir pour objectif la prise de contrôle, le dysfonctionnement ou la destruction de matériels ou d'infrastructures ; mais il peut également s'agir de parer à des détournements de données et de technologies à des fins opérationnelles, stratégiques ou criminelles.

La cybersécurité peut aussi avoir à répondre aux risques d'espionnage étatique ou industriel, ainsi qu'aux pratiques liées à l'intelligence économique, c'est-à-dire à la collecte et au traitement de données pouvant servir au développement des activités des acteurs économiques, financiers ou civils (hôpitaux, administrations…).

Enfin, elle peut encore permettre de contrer différents types d'activités numériques au service de stratégies d'influence, de désinformation ou de manipulation des opinions publiques étrangères (ex. : lors des échéances électorales des pays démocratiques).

Dans l'environnement numérique, la confrontation prend la forme d'un **conflit de basse intensité** ou d'une guérilla dématérialisée, où lignes de codes et manipulations des *hackers* remplacent l'envoi d'agents ou la conduite d'opérations militaires en territoire étranger. La menace peut ainsi surgir à tout instant et se réaliser sans délai. Son intensité peut varier en fonction de l'objet, de l'ampleur ou de la finalité de l'attaque ; le ciblage d'infrastructures critiques (installations nucléaires, réseaux énergétiques, aéroports…) pourrait potentiellement avoir des conséquences équivalentes à un acte terroriste ou à un acte de guerre. Ces caractéristiques façonnent les différentes modalités de la cybersécurité, dont l'aspect préventif est essentiel.

Moyens numériques et matériels au service de la cybersécurité

La cybersécurité **doit permettre d'arrêter ou de neutraliser les attaques ou intrusions potentielles**. La protection des données et des dispositifs numériques par la seule technique du cryptage ne suffit pas. Ainsi, la mise en place de pare-feux (*firewalls*) représente un premier niveau de protection des réseaux ou des matériels informatiques, en leur appliquant une politique de sécurité. Des logiciels antivirus permettent pour leur part de détecter et de neutraliser les fichiers, courriels ou autres programmes malveillants (*malware*), à l'instar des chevaux de Troie (*trojan horses*), qui ont pour but d'ouvrir des accès dérobés (*backdoors*) dans un système informatique, des rançongiciels (*ransomware*) qui consistent en

l'envoi d'un logiciel malveillant qui chiffre l'ensemble des données de terminaux ou de logiciels et demande une rançon en échange du mot de passe de déchiffrement, voire de logiciels espions (*spyware*), qui transmettent des données informatiques de façon couverte à l'insu du système ciblé…

Les logiciels antivirus constituent à cet égard un moyen de contrer le hameçonnage (ou filoutage, dénommé « *phishing* » en anglais), pratique répandue qui permet le détournement d'informations voire une usurpation d'identité électronique (*spoofing*), à partir par exemple d'un geste aussi anodin que l'ouverture d'un fichier infecté, joint à un courriel frauduleux.

La recherche des bogues informatiques (chasse aux bogues ou *bug bounty*), susceptibles de constituer autant de failles ou de vulnérabilités potentielles dans les systèmes informatiques, les logiciels ou les sites Internet, constitue également une mesure de prévention essentielle.

Mais la démarche de prévention peut également s'exercer dès la conception des matériels ou logiciels, dans une approche dite de **« sécurité par conception »** (*security by design*) : il s'agit de déployer nativement les parades nécessaires pour se protéger contre d'éventuelles cyberattaques. Cette recherche d'une anticipation des menaces rencontre néanmoins toujours des limites face à la sophistication croissante des moyens offensifs.

La **protection des chaînes de production de composants essentiels au fonctionnement de certains matériels** participe également à la cybersécurité. Ainsi, la loi de programmation militaire (LPM) française classe dans une catégorie d'« opérateurs d'importance vitale » un certain nombre d'entreprises (alimentation, santé, gestion de l'eau, énergie, transports, activités militaires, industrie, communications électroniques, audiovisuel et information, etc.), dont la production est soumise à des normes particulièrement strictes. Et, lorsque l'usage de matériels, composants et logiciels informatiques étrangers, demeure incontournable, il convient alors de procéder à des travaux de rétro-ingénierie, pour vérifier qu'ils ne recèlent pas de failles ou de vulnérabilités cachées. Pour couvrir l'ensemble des menaces auxquelles la cybersécurité doit répondre, la loi de programmation militaire a également demandé aux opérateurs d'importance vitale de renforcer la sécurité de leurs systèmes d'information. Au niveau de l'UE, le recensement et la désignation des infrastructures critiques européennes [directive 2008/114/CE du Conseil du 8 décembre 2008,

abrogée par la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022] et la mise en place d'un cadre de certification de cybersécurité [règlement cybersécurité (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019] incluant les institutions européennes [règlement (UE/Euratom) 2023/2841 du Parlement européen et du Conseil du 13 décembre 2023] constituent des avancées complémentaires significatives.

On mesure combien la cybersécurité dépend alors du **niveau d'autonomie** dont dispose un État vis-à-vis de matériels et logiciels étrangers : en effet, plus la dépendance technologique d'un État est importante, et plus il devient difficile de garantir l'efficacité des mesures de cybersécurité. Ainsi, dans le cadre de l'initiative « semi-conducteurs pour l'Europe », l'UE a par exemple décidé en 2023 de mobiliser 43 milliards d'euros d'investissements publics et privés. De même, nombre d'États européens limitent la participation de certains opérateurs étrangers (chinois notamment) à la fourniture de technologies alimentant le cœur de leur réseau 5G (composants critiques). En matière de cybersécurité, la souveraineté représente donc un enjeu essentiel. Si elle ne peut être atteinte intégralement au niveau national, il convient de l'envisager à un niveau régional (européen par exemple).

Moyens normatifs au service de la cybersécurité

Enfin, la cybersécurité passe aussi par l'action d'**institutions** et la conclusion d'**accords internationaux**. La France dispose par exemple de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), instituée par le décret n° 2009-834 du 7 juillet 2009 et dont les missions ont été complétées par la LPM n° 2018-607 du 13 juillet 2018 pour les années 2019 à 2025 ; par ailleurs, depuis près de dix ans, elle a développé une quatrième branche de son armée consacrée à la cyberdéfense avec un commandement de la cyberdéfense (Comcyber) à sa tête (décret n° 2017-743 du 4 mai 2017). L'Organisation européenne de cybersécurité (ECSO), instituée en 2016, veille pour sa part à la sécurité des réseaux et de l'information au niveau de l'UE. La réglementation européenne précitée, à laquelle on ajoutera la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 [qui abroge la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016], fixent un certain nombre de règles communes et organisent la coopération des États membres de l'Union. **La Convention (dite « de Budapest ») du Conseil**

de l'Europe du 23 novembre 2001 sur la cybercriminalité participe également à cette évolution du cadre normatif en matière de cybersécurité à l'échelle continentale : il s'agit de la première convention internationale consacrée à la lutte contre ce type de criminalité. Son premier protocole additionnel vise à incriminer la diffusion de matériel ou de propos racistes et xénophobes *via* Internet, et le deuxième, à mettre en place des règles communes en matière de coopération internationale pour la collecte de preuves sous forme électronique aux fins d'enquêtes et de poursuites pénales.

Plus récemment, le 16 octobre 2023, la France, le Monténégro et la Slovénie ont signé à Tirana (Albanie) un accord portant création du Centre de développement des capacités cyber dans les Balkans occidentaux (C3BO), dont le projet de loi déposé au Sénat le 27 novembre 2024 prévoit l'autorisation d'approbation.