

Les nouveaux guerriers chinois de l'information : l'émergence de la Force de soutien à l'information

Joel Wuthnow | 17 octobre 2024



Cet article est une traduction de l'article [« China's New Info Warriors: The Information Support Force Emerges »](#), publié sur War On The Rocks le 24 juin 2024.

Xi Jinping a récemment tenté de [remodeler l'Armée populaire de libération](#) (APL), mais il a finalement été contraint de revenir sur une partie de son œuvre. En avril, l'armée chinoise a connu sa plus grande réorganisation de la décennie, avec la suppression de la Force de soutien stratégique (SSF) et l'inauguration d'une nouvelle Force de soutien à l'information (ISF). Xi a [salué](#) la nouvelle force comme une « force stratégique et un soutien clé pour la coordination de la construction et de l'application des systèmes d'information en réseau ». Il a ajouté qu'elle contribuerait à « fluidifier les liens d'information », à « renforcer la protection de l'information » et à « mettre en œuvre efficacement le soutien à l'information », autant d'éléments cruciaux pour permettre à l'armée de mener des opérations conjointes multi-domaines.

Cette dernière réorganisation laisse néanmoins entrevoir une combinaison de frustration et d'ambition pour les dirigeants chinois. La création de la SSF était un [élément clé](#) des [réformes militaires de Xi en 2015](#) et aurait pu faire partie de son héritage en tant que leader de la plus grande transformation de l'APL en temps de paix. Pourtant, sa suppression après seulement huit ans et demi a indiqué que Xi était prêt à échanger cette réalisation contre un nouvel arrangement qui préparerait certainement mieux l'APL aux conflits régionaux, en particulier aux opérations conjointes de haute intensité nécessaires pour intimider et, si nécessaire, conquérir Taïwan. En effet, des sources chinoises décrivent les réformes comme contribuant à maintenir l'APL sur la voie de son objectif de modernisation pour 2027, qui se concentre sur les préparatifs d'un conflit entre les deux rives du détroit.

Alors que la nécessité d'une réforme suggère de résoudre un problème bien perçu par les autorités, la préoccupation actuelle est que ces changements structurels accroissent la confiance de Xi dans son armée sur le long terme. En effet, l'ISF sera chargée de protéger les systèmes d'information militaire de la Chine contre les attaques de cyberguerre et de guerre électronique et de moderniser les systèmes de commandement et de contrôle afin de mieux exploiter l'intelligence artificielle, améliorant ainsi la rapidité et la précision de la prise de décision chinoise. En fait, cette certitude que l'armée chinoise est désormais mieux organisée, qu'elle dispose de ressources plus importantes et est incitée à poursuivre ces améliorations, pourrait compliquer la dissuasion en affaiblissant les avantages des États-Unis en matière de commandement et de contrôle (C2) interarmées dans tous les domaines, et en réduisant la capacité de Washington à mettre en péril les systèmes chinois. En réponse, de nouveaux investissements tant capacitaires que dans la doctrine américaine seront nécessaires pour s'assurer que les dirigeants chinois restent méfiants quant à leur état de préparation en 2027 et au-delà.

Soutien à l'information

La doctrine militaire chinoise soutient depuis longtemps que l'issue des guerres de haute intensité sera déterminée par un [concours entre systèmes opposés](#), parfois appelé « confrontation des systèmes » ou guerre de « destruction des systèmes ». Pour l'emporter, le vainqueur doit non seulement être en mesure de détruire les systèmes critiques de son adversaire, tels que la logistique, les communications, les nœuds de C2, les porte-avions, mais aussi de protéger ses propres systèmes. Depuis le début des années 2000, les écrits doctrinaux évoquent donc la nécessité de mettre en place un « système de soutien à l'information » capable de permettre à une force interarmées de communiquer efficacement en temps de guerre en maintenant les réseaux de combat, en transmettant et en traitant les données et en protégeant les systèmes critiques contre les attaques de cyberguerre et de guerre électronique adversaires.

Dans les années 2010, les sources chinoises ont souvent discuté de ces exigences sous l'étiquette du renforcement des « systèmes d'information en réseau ». Le Science of Military Strategy de 2015, un manuel clé pour les officiers chinois, a appelé l'armée à « améliorer continuellement les capacités de combat interarmées basées sur les systèmes d'information en réseau » et à « jouer pleinement le rôle de la technologie de l'information ». Une révision de ce volume en 2017 est allée plus loin, en décrivant ce type d'opération comme rien de moins que la « forme de base du combat ». Ce point de vue a été [approuvé](#) par le 19^e Congrès du Parti en octobre 2017, qui a chargé l'armée d'« augmenter les capacités de combat conjointes basées sur les systèmes d'information en réseau », un objectif [réitéré](#) lors du 20^e Congrès du Parti cinq ans plus tard.

Au cours de cette période, l'armée a expérimenté la meilleure façon d'institutionnaliser l'accent mis par la doctrine sur le soutien à l'information. Avant l'ère Xi, les responsabilités en matière de systèmes d'information, de communications et de réseaux de C2 étaient assumées par le département de l'informatisation de l'ancien département de l'état-major général (le *General Staff Department's Informatization Department*). Après les réformes de 2015-2016, cette fonction a été transférée au nouveau département de l'état-major interarmées sous le nom de Base de soutien de l'information. Lors d'une autre réorganisation effectuée en 2017-2019, cette organisation a été transférée dans la la SSF sous le nom de Base de communication de l'information. Selon J. Michael Dahm, cette organisation contrôlait diverses [brigades de communication de l'information](#) au sein des cinq commandements de théâtre.

Autre innovation, en 2017 : un nouveau « groupe d'opérations d'information » a été [révélé](#) lors du défilé du 90^e anniversaire de l'APL. Dirigé par un général de division, ce groupe affilié à la SSF comprenait une « équipe de soutien à l'information », ainsi que des formations de reconnaissance électronique, de contre-mesures électroniques et de systèmes aériens sans équipage. Un analyste chinois s'est [vanté](#) de l'amélioration des « groupes d'information de combat et des capacités de guerre électronique », attestant que « dans les futures guerres locales dans des conditions de haute technologie, nous devrions gagner ». Néanmoins, les références à ce « groupe » ont diminué, remplacé dans les années 2020 par une nouvelle « force de technologie de l'information », dont les [annonces de recrutement](#) ciblant les étudiants des universités d'élite indiquaient qu'elle était « principalement responsable des tâches de soutien des informations de réseau et de protection de la sécurité de l'information ».

L'impulsion de la réforme

Plusieurs facteurs ont pu contribuer à la décision de créer une nouvelle force de soutien à l'information. Tout d'abord, les analystes chinois ont prêté une attention particulière aux améliorations apportées aux systèmes de soutien à l'information des États-Unis au cours de la décennie précédente. Ils ont été particulièrement intéressés par l'annonce faite en 2012 par la *Defense Information Systems Agency* d'un programme d'environnement d'information conjoint ([Joint Information Environment](#)) visant à faire converger « les communications, l'informatique et les services d'entreprise vers une plateforme conjointe unique pouvant être exploitée pour toutes les missions du département ». Ils ont également observé la révélation du concept de C2 interarmées tous domaines à la fin des années 2010, selon lequel l'agence [fournirait aux décideurs](#) des « données correctes pour les aider à

prendre des décisions éclairées en temps réel », ainsi que d'autres innovations telles que l'utilisation de drones pour fournir des [communications protégées et sécurisées sur le champ de bataille](#).

Deuxièmement, la piètre performance de la Russie dans le conflit ukrainien a démontré les risques liés à l'absence d'un soutien efficace en matière d'information sur le champ de bataille. Une analyse de l'industrie de la défense chinoise a expliqué que la Russie était historiquement faible dans ce domaine, depuis la Seconde Guerre mondiale, lorsque les chars soviétiques manquaient d'équipement de communication et étaient facilement isolés et détruits par les batteries antichars allemandes. Cette faiblesse a persisté en Ukraine, où l'auteur note que l'armée russe n'a pas détruit l'infrastructure civile de communication de l'Ukraine parce qu'elle avait besoin de ces systèmes pour coordonner ses propres forces. Cela a créé de sérieuses vulnérabilités car les défenseurs ukrainiens pouvaient surveiller les communications, y compris entre les généraux russes de haut rang opérant près des lignes de front, ce qui a entraîné la perte de plusieurs de ces commandants.

Troisièmement, dans ce contexte des améliorations américaines et des échecs russes, les analystes chinois ont observé les limites de leurs propres systèmes. Un article paru en 2018 dans le *PLA Daily* [fait allusion](#) aux « obstacles conceptuels, organisationnels et techniques » qui entravent le fonctionnement des systèmes d'information de réseau de la Chine. L'armée devrait se concentrer davantage sur « l'unification des normes de données, des liens clés, des règles de fonctionnement et des informations de base ». Comme l'écrit Samuel Bresnick dans un [nouveau rapport](#), d'autres sources chinoises ont fait état de difficultés à maintenir des réseaux sécurisés et à maintenir « les communications dans les futurs conflits de haute intensité ». Un colonel de haut rang commentant la justification de la réforme de 2024 a noté la [persistance de problèmes](#) tels que « l'incompatibilité des logiciels et du matériel » entre les différents services et le faible partage d'informations entre les unités. Selon lui, la nouvelle ISF « établira une solide ligne de défense dans ce domaine et assurera la supériorité en matière d'information ».

Quatrièmement, il a donné des instructions plus fermes à l'APL pour qu'elle se prépare à des missions militaires de haut niveau. Plus précisément, M. Xi [aurait demandé à l'armée d'être capable de vaincre Taïwan d'ici 2027](#), dans le cadre d'une [stratégie de développement](#) actualisée annoncée en 2020. On peut supposer que la nécessité pour Xi d'annoncer cet objectif reposait sur l'observation du retard pris par l'armée dans sa préparation. Les réformateurs auraient examiné de près les domaines dans lesquels des améliorations institutionnelles et techniques étaient nécessaires, notamment dans le domaine du soutien à l'information, dont le fonctionnement serait essentiel à la « domination de l'information » dans toute lutte contre Taïwan et les États-Unis. Les commentaires chinois [ont salué](#) la nouvelle force comme un « progrès important dans l'augmentation de l'efficacité de l'armée au combat » qui « aiderait certainement » à atteindre l'objectif de 2027 « dans les délais prévus ».

Amélioration des systèmes

En tant qu'innovation institutionnelle, la Force de soutien à l'information pourrait renforcer la confiance des dirigeants dans la poursuite d'une « guerre de destruction des systèmes » en intégrant davantage les capacités de combat interarmées « basées sur des systèmes d'information en réseau ». Cet objectif n'est pas nouveau, mais le nouvel arrangement pourrait présenter des avantages par rapport à ses prédécesseurs. La force de soutien à l'information, qui n'est plus enfouie dans les départements généraux ou la force de soutien stratégique, ainsi que d'autres forces de soutien existantes, notamment la force du cyberspace, responsable de la guerre cybernétique et électronique offensive, la force spatiale et la force de soutien logistique interarmées, sont placées sous la supervision directe de la Commission militaire centrale et peuvent recevoir des conseils de Xi et de ses hauts gradés. Cela permet de [résoudre un problème de bureaucratie excessive](#) qui empêchait les forces de « s'adapter à un environnement en constante évolution ».

Les changements de statut de la nouvelle force lui confèrent également des avantages bureaucratiques. Contrairement à son prédécesseur, qui était probablement d'un grade inférieur, la nouvelle ISF est désormais un service de niveau *Deputy Theater Command Leader*, comme les autres forces de soutien. Cela signifie qu'elle est relativement haut placée dans la hiérarchie organisationnelle de l'armée et que, grâce à son accès direct à la Commission militaire centrale (CMC), elle est mieux placée pour réclamer les ressources dont elle a besoin pour mener à bien sa mission. Cependant, elle n'est pas trop haut placée sur le plan bureaucratique – elle se situe toujours un niveau en dessous des cinq commandements de théâtre. Il sera donc difficile pour la force de se transformer en un centre de pouvoir cloîtré (et potentiellement corrompu), oublieux des directives de niveau supérieur, telles que celles du département de l'état-major interarmées et des théâtres d'opérations, qui devront coordonner son développement et ses opérations.

La mission de la nouvelle force, qui consiste à intégrer les capacités de combat interarmées, incombera à ses nouveaux dirigeants. Le premier commandant, le [lieutenant-général Bi Yi](#), est un officier de carrière des forces terrestres (PLAGF) qui a

passé la majeure partie de sa carrière au sein du commandement du théâtre nord. Ses qualifications découlent principalement de son poste précédent de directeur adjoint du département de formation et de gestion de la CMC, qui est responsable de la définition des besoins de formation interarmées – ce qui le place dans une position idéale pour comprendre le rôle que les systèmes d'information doivent jouer dans les exercices interarmées – ainsi que de son rôle précédent de commandant adjoint de la SSF. Le nouveau commissaire politique, le [général Li Wei](#), a précédemment servi dans la région militaire de Nanjing (responsable de Taïwan) et a le statut d'officier de commandement de théâtre, ce qui lui confère un avantage en matière de lobbying au nom de la force.

Un avenir incertain

La création de la ISF suggère que l'armée chinoise continue d'étudier et de mettre à jour son organisation lorsqu'elle en a besoin. Xi Jinping semble ne pas être satisfait du fonctionnement de l'ancienne SSF, et a accepté des conseils militaires qui ont éliminé une bureaucratie entière pratiquement du jour au lendemain et en ont créé une nouvelle, même si ce n'était pas à partir de rien. Cette décision donne une image de frustration, d'une part, mais aussi de capacité d'adaptation, d'autre part. Une partie des réformes militaires initiales de Xi n'a pas atteint son objectif, mais de nouvelles idées – probablement inspirées par une combinaison de ce que les États-Unis avaient fait de bien, de ce que la Russie avait fait de mal et des besoins spécifiques de l'armée chinoise – ont été en mesure de gagner le soutien de Xi. L'adaptation institutionnelle, avec une finalité pratique en vue, était pour lui une priorité plus importante que la consolidation de l'une de ses principales réalisations de 2015 et 2016.

Si elle réussit ses missions, l'ISF permettra à l'armée chinoise d'être plus compétitive dans la « guerre de destruction des systèmes ». Les différentes armées, services et branches pourront se coordonner plus facilement, les adversaires auront moins d'options pour infiltrer et attaquer les systèmes d'information critiques des réseaux, et les améliorations techniques permettront aux commandants de tirer parti de la [puissance de l'intelligence artificielle](#) pour comprendre et agir sur des quantités massives de données dans un délai réduit. Si cela fonctionne, les commandants en chef et même Xi lui-même, qui se trouve directement au-dessus de cette force, auront davantage confiance dans la capacité de l'APL à réussir dans une situation d'urgence face à un adversaire bien préparé, évitant ainsi le sort de leurs frères russes. Il pourrait en résulter une conviction plus forte que les forces militaires chinoises ont respecté le délai de 2027 pour être mieux à même de faire la guerre de l'autre côté du détroit de Taïwan.

Toutefois, l'efficacité de la force dépendra de plusieurs incertitudes majeures. Premièrement, de sa capacité à approfondir l'interopérabilité entre les services, ce qui a échappé aux réformes précédentes. Deuxièmement, de sa capacité à soutenir les utilisateurs finaux. Pour prouver sa valeur, la force devra travailler en étroite collaboration avec les commandements soutenus, tout comme l'Agence des systèmes d'information de la défense offre un soutien au niveau de l'entreprise aux commandements de combat géographiques et fonctionnels par l'intermédiaire de ses [bureaux locaux](#). Cependant, la manière dont la force coordonnera ses activités avec la Commission militaire centrale, les services et les théâtres d'opérations n'est pas encore claire. On ne sait pas non plus si et dans quelle mesure elle soutiendra les opérations mondiales, ce qui pourrait inclure la gestion des communications par satellite et des satellites de navigation Beidou. Troisièmement, de sa capacité, face à la concurrence des entreprises privées, à recruter les talents civils dont elle a besoin pour accomplir des tâches telles que l'ingénierie logicielle, l'intégration de l'intelligence artificielle et le développement de nouveaux modes de communication et de cryptage. Enfin, la dernière variable et la plus importante, est de savoir si l'APL peut suivre le rythme des avancées techniques américaines. D'une part, les réformes rappellent que la recherche d'un C2 interarmées dans tous les domaines ne se fait pas en vase clos. Les adversaires conçoivent et améliorent leurs propres approches. Le camp le mieux à même de tirer parti de l'intelligence artificielle et d'autres nouvelles technologies pourrait obtenir un [avantage décisif](#) – et être plus confiant dans l'utilisation de la force en premier lieu. Les États-Unis ont peut-être pris une longueur d'avance, mais la question de savoir s'ils peuvent conserver cette avance ne peut pas être considérée comme acquise, et devrait donc rester une priorité pour le ministère de la défense ainsi que pour les alliés des États-Unis dans l'Indo-Pacifique (qui travaillent à la mise en place d'un [système combiné de commandement et de contrôle](#) interarmées plus performant).

La question se pose également de savoir si les États-Unis peuvent renforcer la dissuasion. La mise en péril des systèmes d'information chinois pourrait placer Pékin devant de [graves dilemmes opérationnels](#) et favoriser la dissuasion – ce point est au cœur de la réflexion de l'armée américaine sur la mise en œuvre de sa propre version de la « guerre de destruction des systèmes ». Le ministère de la défense réalise de nouveaux investissements dans la [guerre électronique](#). Les budgets consacrés aux cyber-opérations [augmentent](#) également et soutiennent de nouveaux dispositifs tels que le groupe de résultats sur la Chine ([China Outcomes Group](#)) du U.S. Cyber Command. Néanmoins, pour renforcer la dissuasion, il faudra tout d'abord comprendre les mécanismes du nouveau système chinois, ce qui nécessite une analyse plus approfondie des liens de communication qui assurent la cohésion du système. Il faudra également investir davantage dans les outils nécessaires pour cibler ces systèmes, y compris l'aptitude à [reconstituer rapidement](#) les capacités de guerre cybernétique et électronique dans un environnement

dégradé. Enfin, la doctrine américaine doit s'adapter à l'évolution de la structure de l'adversaire, notamment en identifiant les principales vulnérabilités du nouveau système et en élaborant une campagne visant à révéler certaines capacités américaines susceptibles de perturber l'aptitude de la Chine à maintenir des systèmes d'information militaires résistants en temps de guerre. Ces mesures seront nécessaires pour saper la confiance que Xi et son général en chef ont pu retirer de la dernière réorganisation.

Crédits photo : War On the Rocks



Joel Wuthnow

Le Dr Joel Wuthnow (@jwuthnow) est chercheur associé au Center for the Study of Chinese Military Affairs de la U.S. National Defense University. Cet article ne représente que son point de vue et non celui de la National Defense University, du ministère de la Défense ou du gouvernement américain.

Comment citer cette publication

Joel Wuthnow, « Les nouveaux guerriers chinois de l'information : l'émergence de la Force de soutien à l'information », *Le Rubicon*, 17 octobre 2024
[<https://lerubicon.org/les-nouveaux-guerriers-chinois-de-linformation-lemergence-de-la-force-de-soutien-a-linformation/>].

