

Appel à communications :
Journée d'étude du CIENS (ENS-PSL)

**« Le rôle du cyber dans les conflits contemporains.
Quelle place dans l'escalade ?**

Quelle articulation avec les autres domaines de la conflictualité ? »

Judi 19 mars de 9h à 18h30
Salle des Actes à l'ENS
45 rue d'Ulm, 75005 Paris

Argumentaire et état de l'art

La guerre lancée par la Russie en plein cœur de l'Europe le 24 février 2022 et les foyers de crises de l'Asie et du Moyen-Orient, marqués par la confrontation entre Israël et l'Iran¹, l'Inde et le Pakistan², et Taïwan et la Chine, montrent que **la conflictualité cyber, généralement considérée comme étant sous le seuil de la guerre, occupe désormais une place majeure dans les guerres dites de « haute intensité³ » et dans les crises internationales contemporaines, y compris à dimension nucléaire.** Le cyber y vient notamment soutenir ou entraver des manœuvres de guerre conventionnelle grâce, par exemple, au piratage ou à la défense cyber de drones sur des terrains de conflits largement « dronisés⁴ », à des opérations dans le champ électromagnétique⁵ ou encore dans le domaine des télécommunications numériques satellitaires⁶.

¹ Israël et l'Iran se sont livrés à de multiples cyberattaques dans le cadre d'un conflit qui s'est structuré autour du programme nucléaire iranien en juin 2025, dit « Guerre des douze jours ». Amaëlle GUITON, « Guerre cyber. Le cyberspace, autre front de la guerre entre Israël et l'Iran », *Libération*, 20 juin 2025.

² Carla B., *RAPPORT : Tensions entre l'Inde et le Pakistan (avril-mai 2025)*, SysDream, 24 juillet 2025. URL : <https://sysdream.com/blog/rapport-tensions-entre-linde-et-le-pakistan-avril-mai-2025/>.

³ Sur ce concept, utilisé ici par commodité, lire Jean-Baptiste JEANGÈNE VILMER, « La haute intensité : limites du concept et implications pour la France », *Le Rubicon*, 30 juin 2022, qui met en évidence la signification mouvante de ce concept « ancien, d'origine britannique, qui a été adopté aux États-Unis et à l'OTAN dans les années 1970 » pour désigner une hypothétique « Troisième Guerre mondiale » qui prendrait la forme d'une « guerre nucléaire entre l'OTAN et le Pacte de Varsovie. ». Après la Guerre froide et la fin des grands blocs stratégiques, puis l'émergence d'une multipolarisation de la scène internationale, il a été considéré comme caduc, car inadapté à la description d'« une réalité plus complexe » où la conflictualité armée et les crises prenaient des formes non étatiques. Il a été repris en France au début des années 2020 pour désigner « un affrontement en raison d'enjeux jugés majeurs, voire existentiels ; dans plusieurs domaines en même temps, y compris non militaires ; avec une grande violence et des pertes élevées. ».

⁴ David KAUFMANN et Pierre CASANOVA, « Dronisation et robotisation du champ de bataille », *Servir*, n°525, 2024, p. 16-20 et Vincent TOURET, « Désigne, détruit, domine : la dronisation massive des opérations comme potentielle révolution militaire », *Notes de l'Ifri*, Ifri, juin 2025.

⁵ Éric GOMEZ, « Focus 2. La guerre électronique », *Les guerres de l'information à l'ère numérique*, PUF, 2021, p. 79-85.

⁶ Le piratage du réseau de Viasat, une entreprise de télécommunication étatsunienne exploitant KA-SAT (un satellite opéré par l'entreprise européenne Eutelsat) en est l'exemple le plus emblématique. Béatrice HAINAUT, « Guerre dans l'espace : de l'ombre à la lumière », *Inflexions*, vol. 56, n°2, 2024, p. 30-31 ; Stéphane TAILLAT, Didier DANET et Amaël CATTARUZZA, « Conclusion. La cyberdéfense après la guerre en Ukraine », dans S. Taillat, D. Danet, A. Cattaruzza (dir.), *La Cyberdéfense : Politique de l'espace numérique*, Armand Colin, 2023, p. 269-278.

Ce constat de l'omniprésence de la conflictualité cyber dans les guerres et les crises actuelles a été précédé d'**une vingtaine d'années de réflexion et de discussions au sujet de la place que devrait avoir le domaine cyber dans les doctrines stratégiques des États**. En France, le cyber a été considéré d'abord comme un outil à usage ponctuel relevant des pratiques clandestines et du renseignement⁷, puis comme un outil d'épaullement des forces armées dans le conflit⁸. Du point de vue de la doctrine française, le domaine cyber reste donc distinct de la dissuasion qui est par définition nucléaire, comme le rappelle la *Revue stratégique de cyberdéfense* du Secrétariat général de la défense et la sécurité nationale (SGDSN) publiée le 12 février 2018, qui affirme : « La France réserve, quant à elle, le terme de dissuasion au domaine nucléaire militaire. [...] La dissuasion se fonde sur la nature unique de l'arme nucléaire. [...] La "grammaire" de la dissuasion nucléaire est singulière et ne s'applique pas aux actions cybernétiques⁹ ». Aux États-Unis toutefois, le concept de dissuasion est plus malléable, ce qui a donné lieu à une importante réflexion autour des conditions de possibilité d'une « *cyber-deterrence*¹⁰ » entre le début des années 2000 et la fin des années 2010. Cette *cyber-deterrence* a généralement été définie comme une stratégie visant à décourager les attaques informatiques d'États adverses en les menaçant de représailles proportionnées, ou en rendant les coûts potentiels de leurs attaques supérieurs aux bénéfices qu'ils pouvaient escompter en tirer.

Cependant, **ce débat sur la *cyber-deterrence* a aujourd'hui largement perdu de son acuité**. Les nombreuses tentatives de la littérature en études stratégiques et science politique pour penser les modalités d'une telle *dissuasion cyber* ont montré qu'elle se heurtait en effet à de nombreuses limites, aussi bien conceptuelles que techniques, depuis la difficulté d'attribution des attaques¹¹ à l'impossibilité de garantir leurs effets¹², la répétition à l'identique de leurs effets¹³ ou leurs conséquences politiques, diplomatiques et

⁷ « Les opérations ciblées conduites par les forces spéciales et les frappes à distance, le cas échéant cybernétiques, pourraient devenir plus fréquentes, compte tenu de leur souplesse d'emploi dans un contexte où les interventions classiques continueront d'être politiquement plus difficiles et parfois moins efficaces. », MINISTÈRE DE LA DÉFENSE, *Livre blanc sur la défense et la sécurité nationale 2013*, 29 avril 2013, p. 30.

⁸ « Les Armées intègrent désormais le combat cybernétique comme un mode d'action à part entière dont les effets se combinent aux autres dans une manœuvre globale. », RÉSERVE CITOYENNE DU GOUVERNEUR MILITAIRE DE PARIS, « Les Conférences de la RC : retour sur le thème du mardi 16 novembre 2021. », <https://www.reserve-citoyenne-paris.org/2021/11/les-conferences-de-la-rc-retour-sur-le-theme-du-mardi-16-novembre-2021.html> et site web du Ministère des Armées, <https://www.defense.gouv.fr/nos-expertises/cyberdefense-au-ministere-armees-anciens-combattants>.

⁹ SGDSN, *Revue stratégique de cyberdéfense*, p. 37. L'actualisation de la *Revue nationale stratégique* du SGDSN en juillet 2025 ne revient pas sur ce principe, sans toutefois le réitérer explicitement.

¹⁰ Joseph S. NYE, « Nuclear Lessons for Cyber Security », *Strategic Studies Quarterly*, 2011, p. 18-38 ; « Deterrence and Dissuasion in Cyberspace », *International Security*, vol. 41, n°3, 2016, p. 54-63 ; « From bombs to bytes: Can our nuclear history inform our cyber future? », *Bulletin of the Atomic Scientists*, vol. 69, n°5, 2013, p. 8-14 ; Martin C. LIBICKI, *Cyberdeterrence and cyberwar*, RAND Corporation, 2009.

¹¹ Martin C. LIBICKI, *op. cit.*, § « Cyberdeterrence May Not Work as Well as Nuclear Deterrence », RAND Corporation, 2009, p. XVI.

¹² Martin C. LIBICKI, *op. cit.*, § « Defining Cyberdeterrence », p. 31 et chap. III « Why Cyberdeterrence Is Different », § « If Retaliation Does Not Deter, Can It at Least Disarm? », p. 59-62.

¹³ Martin C. LIBICKI, *op. cit.*, chap. III, § « Can We Do So Repeatedly? », p. 56-57.

militaires¹⁴, en passant par l'intrication des infrastructures numériques des États à l'échelle mondiale¹⁵ : autant de conditions qui doivent faire l'objet de certitudes pour établir la crédibilité d'une capacité dissuasive, qui ne peut donc pas être garantie dans le domaine cyber¹⁶.

Parallèlement, **la conflictualité cyber démontre *re vera* que le cyber était un domaine d'emploi permanent**, y compris dans ses formes les plus incapacitantes et potentiellement destructrices. Les nombreuses cyberattaques menées par des États contre des systèmes industriels et énergétiques parfois stratégiques, depuis *Olympic Games*¹⁷ jusqu'aux multiples cyberattaques observées dans le cadre de la guerre de grande ampleur de la Russie en Ukraine, l'indiquent. Aujourd'hui, il est donc clair que, dans le domaine cyber, la logique dissuasive est résiduelle¹⁸.

La place grandissante prise par le cyber dans les conflits doit ainsi nous amener à **réinterroger son rôle dans les dynamiques d'escalade et de dissuasion *avant et pendant* les guerres et crises, y compris celles qui comprennent une dimension nucléaire.**

Quatre questions principales seront par conséquent explorées durant cette journée d'étude :

- 1. Les caractéristiques de la conflictualité cyber évoluent-elles en fonction des différentes phases du conflit (paix, crise, guerre) ?**
- 2. Existe-t-il une dynamique d'escalade spécifique au domaine cyber ? Quelles en sont les caractéristiques ?**
- 3. Comment la dimension cyber de la conflictualité interagit-elle avec les autres domaines du conflit ? Ces interactions modifient-elles les dynamiques et les risques d'escalade d'ensemble ?**

¹⁴ Martin C. LIBICKI, *op. cit.*, chap. III, § « Will Third Parties Join the Fight? », p. 62-63 et « Does Retaliation Send the Right Message to Our Own Side? », p. 64-65, chap. V « A Strategy of Response », § « Should Deterrence Be Extended to Friends? », p. 104-106.

¹⁵ Richard A. CLARK, Robert K. KNAKE, *Cyber War: The Next Threat to National Security and What to Do About It*, HarperCollins, New York, 2010, p. 189 et Joseph S. NYE, « Deterrence and Dissuasion in Cyberspace », art. cit., p. 45.

¹⁶ Les liens infrastructurels entre l'Internet russe et l'Internet ukrainien n'ont, par exemple, pas empêché la Russie de mener une cyberattaque aussi destructrice que celle utilisant le *wiper* NotPetya contre l'Ukraine en 2017, au risque de subir, par effet de contagion, les mêmes destructions de données sur son propre réseau. Voir Andy GREENBERG, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*, « Part IV - Apotheosis », chap. 24 « NotPetya », Doubleday, New York, 2019, p. 194.

¹⁷ L'opération israélo-étatsunienne a employé le programme malveillant Stuxnet contre la centrale iranienne de Natanz dédiée à l'enrichissement de l'uranium entre 2006 et 2012.

¹⁸ Noter cependant que, selon certains analystes, l'usage de différents types d'intelligence artificielle dans les domaines du nucléaire militaire et de la cybersécurité / cyberdéfense, aussi bien sur le plan défensif que du point de vue offensif, indique que la question d'une dissuasion cyber pourrait se poser à l'avenir. Vladislav CHERNAVSKIKH et Jules PALAYER, *Impact of Military Artificial Intelligence on Nuclear Escalation Risk*, SIPRI, juin 2025.

4. Dans quelles conditions (ruptures technologiques, reconfiguration du système international etc.) non encore advenues le cyber pourrait-il être vecteur d'une fragilisation du paradigme de la dissuasion nucléaire¹⁹ ?

Objectifs

La généralisation de la conflictualité cyber, la démultiplication de ses effets possibles par l'Intelligence Artificielle (IA) et son articulation avec d'autres innovations technologiques telles que les drones ou les réseaux satellitaires du *New Space*, viennent potentiellement bouleverser les logiques de maîtrise de l'escalade. Cette journée d'étude vise donc à alimenter la réflexion sur la *grammaire* de la conflictualité cyber et sur les *dynamiques d'escalade* qui la caractérisent, à un moment où une guerre « de haute intensité », marquée à la fois par un important usage du cyber et par la prégnance d'un rapport des forces entre puissances fondé sur la dissuasion nucléaire, fait rage en Europe.

Alors que les évolutions récentes de la conflictualité ont plutôt renforcé l'écart entre les logiques régissant le cyber et celles de la dissuasion, l'objectif de la journée d'étude est d'élucider la manière dont les différences entre les grammaires des domaines de la conflictualité (cyber, conventionnel, spatial, informationnel, jusqu'à celui de la dissuasion nucléaire) pourraient conduire à une escalade involontaire et non maîtrisée si elles n'étaient pas suffisamment pensées, ou à l'inverse, permettre un contrôle de l'escalade plus efficace ; notamment si les grammaires propres au cyber et à d'autres domaines étaient articulées et faisaient l'objet d'une approche d'ensemble.

Thématiques

Nous invitons les doctorants, chercheurs, universitaires et professionnels à soumettre des propositions de communication sur les thématiques suivantes (liste non exhaustive) :

- **Le domaine cyber : ajout d'une dynamique escalatoire non maîtrisée dans les conflits ou outil contribuant à leur maîtrise ?**
 - Le cyber comme élément d'« hybridité » est-il facteur d'escalade non contrôlée ou de maîtrise de l'escalade (en maintenant le conflit « sous le seuil » de la guerre) ? (*études de cas et analyses*)
 - Les cyberattaques contre des infrastructures critiques, prémices de la guerre ou moyens de l'éviter (mode de dissuasion, signalement) ? (*études de cas et analyses*)
 - Conflictualité cyber dans l'espace extra-atmosphérique et risques stratégiques (*études de cas et analyses*)

¹⁹ Lire à ce sujet Andrew FUTTER, *Hacking the Bomb: Cyber Threats and Nuclear Weapons*, Georgetown University Press, 2018 et Herbert LIN, *Cyber Threats and Nuclear Weapons*, Stanford University Press, 2021. On peut aussi voir Wan WILFRED, Andraz KASTELIC, Eleanor KRABILL, *The Cyber–Nuclear Nexus: Interactions and Risks. Nuclear Risk Reduction*, « Friction Points Series », n°2, UNIDIR, 2021 et Matt CAYLOR, « The Cyber Threat to Nuclear Deterrence », *War on the Rocks*, 1^{er} février 2016. Dans le champ des études françaises, voir Adrien SCHU, « Dissuasion nucléaire : le cyber comme instrument de contre-force », *Études internationales*, vol. 51, n°2, été 2020.

- Dans quelles conditions le cyber pourrait-il devenir un véritable facteur de dissuasion ? (*études de cas et analyses*)
- **Le rôle de la conflictualité cyber avant la crise ou la guerre :**
 - Les opérations cyber comme outil d'avertissement ou de « signalement » d'un désaccord diplomatique ou militaire (*études de cas et analyses*)
 - Les cyberattaques à la veille du lancement de la guerre de grande ampleur de la Russie en Ukraine : prévention de la guerre ou premières frappes ?
 - Les cyberattaques en amont et au cœur de la crise Israël-Iran (*études de cas et analyses*)
 - Le rôle des cyberattaques dans les tensions entre la Chine et Taïwan autour de la gouvernance du territoire
- **La place de la conflictualité cyber dans les guerres et les conflits dits « de haute intensité » et l'effet des cyberattaques sur la stabilité stratégique aux échelles régionales et internationales :**
 - La conflictualité cyber dans la guerre en Ukraine (*études de cas et analyses*)
 - Conflictualité cyber dans la guerre en Ukraine et risque nucléaire
 - Conflictualité cyber, numérisation et « dronisation » du champ de bataille en Ukraine / Conflictualité cyber et guerre dans le champ électromagnétique (GCEM) en Ukraine
 - Guerre en Ukraine et multiplication des acteurs du conflit cyber en Europe et dans le monde
 - La place de la conflictualité cyber dans les crises et conflits régionaux à dimension nucléaire (*études de cas et analyses*) :
 - au Moyen-Orient : la conflictualité cyber entre Israël et l'Iran et la question de la prolifération nucléaire ; la guerre Iran-Israël et les acteurs de la dimension cyber du conflit
 - dans le conflit Inde-Pakistan, avec des affrontements ouverts entre deux puissances nucléaires dotées de capacités cyber
- **Quelles conséquences et implications pratiques des évolutions de la cyber-conflictualité pour la posture cyber de la France, de l'Union européenne et de l'OTAN ?**
 - L'attribution, un mode de signalement²⁰ ?
 - Les évolutions dans la gestion du dialogue et de l'escalade dans le domaine cyber

Cette journée d'étude s'inscrit dans une démarche pluridisciplinaire et une perspective stratégique. Elle est ouverte à toutes les disciplines techniques et des sciences humaines et

²⁰ L'année 2025 a été marquée par la première attribution publique officielle d'une cyberattaque par la France le 29 avril, à travers la voix de la diplomatie française alors incarnée par Jean-Noël Barrot. Cette cyberattaque advenue en 2017 avait conduit à la fuite des courriels de l'équipe de campagne de l'actuel Président Emmanuel Macron, à l'instigation d'APT28 / *Fancy Bear*, un groupe de cyberattaquants liés au GRU (le renseignement militaire russe). Son attribution a constitué un changement majeur dans les pratiques françaises en matière de dialogue intérieur et international sur la conflictualité cyber entre les États.

sociales. Nous invitons en particulier les doctorants et jeunes chercheurs à soumettre des propositions.

Modalités de soumission

Les propositions de communication doivent inclure un titre, un résumé d'environ 500 mots, ainsi qu'un CV et les coordonnées de l'auteur (nom, affiliation, adresse de courriel). Les propositions doivent être envoyées à ciens@ens.fr et marie-gabrielle.bertran@ens.psl.eu avant le **16/01/2025**.

Une publication collective est envisagée à l'issue de la journée.

Calendrier

Date limite de soumission des propositions : **lundi 16 janvier 2026**

Notification d'acceptation : **samedi 31 janvier 2026**

Journée d'étude : **jeudi 19 mars 2026**

Modalités du déroulement de la journée d'étude :

- les intervenants devront prévoir une intervention orale d'une **durée de 20 minutes** maximum ;
- il sera également demandé aux intervenants de **partager un mois à l'avance avec les autres participants leur présentation au format écrit**, afin de nourrir la réflexion collective sur les thématiques abordées et les échanges durant la journée.

Comité scientifique :

- Kévin Limonier (Professeur, Université Paris 8, co-directeur du projet GEODE)
- Adrien Schu (Professeur junior, Université Paris 2 - Centre Thucydide, directeur de l'AEGES)
- Maïlys Mangin (MCF, Université Toulouse Capitole et chercheuse associée au CIENS)
- Yannick Pincé (MCF, Paris Sorbonne Nouvelle et chercheur associé au CIENS)
- Paul Zajac (expert et chercheur associé au CIENS)
- Guillaume Schlumberger (expert associé au CIENS)
- Laurent Properi (expert associé au CIENS)
- Hugo Zylberberg (consultant en cybersécurité)

Comité d'organisation (équipe du CIENS et pôle cyber du CIENS) :

Marie-Gabrielle Bertran (post-Doc au CIENS), Elsa Novelli (post-Doc au CIENS), Frédéric Gloriant (directeur du CIENS), Stéphanie Braquehais (cheffe de projet du CIENS)