****

**Pall Mall Process**

**Implication du Forum de Paris sur la Paix**

Lors de la conférence de Lancaster House à Londres du 6 et 7 février 2024, la France et le Royaume-Uni ont conjointement lancé le « Pall Mall Process » visant à lutter contre la prolifération et l’usage irresponsable des capacités d’intrusion cyber disponibles sur le marché commercial. Cette initiative « s’appuie sur les discussions tenues lors de l’édition 2023 du Forum de Paris sur la Paix » et s’inscrit dans le prolongement  du travail conduit dans le cadre de l’Appel de Paris pour la confiance et la sécurité dans le cyberespace, dont le principe n°5 appelle à élaborer des moyens d’empêcher la prolifération de logiciels malveillants et de pratiques informatiques destinés à nuire ([communiqué conjoint du 7 février 2024](https://www.gov.uk/government/publications/pall-mall-process-on-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities-uk-and-france-joint-communique/cybersecurity-joint-communique-of-the-united-kingdom-and-france-on-the-lancaster-house-conference-to-tackle-proliferation-and-irresponsible-use-of-co)).

À cette occasion, la prochaine édition du Forum a été désignée comme séquence privilégiée pour organiser la prochaine réunion plénière du processus de Pall Mall, devant être accueillie par la France. Cet acceuil serait d’autant plus logique que ce processus s’inscrit dans la droite ligne du groupe de travail multi-acteurs convoqué dans le cadre de l’Appel de Paris, dont les travaux s’apprêtent à reprendre sur la base de ces dernières avancées. Afin de renforcer la cohérence des différents efforts internationaux et de repositionner l’Appel de Paris, à la source des efforts français en matière de protection d’un cyberespace libre, ouvert, unique et sûr, le Forum propose (1) de s’appuyer sur l’Appel de Paris pour la convocation des réunions intermédiaires du processus de Pall Mall, avant la prochaine réunion annuelle en France et (2) de se fonder sur le groupe de travail de l’Appel de Paris pour recueillir les contributions de la communauté des parties prenantes.

La prochaine édition du Forum a été choisie comme moment idéal pour tenir la prochaine réunion plénière du processus de Pall Mall, qui sera organisée par la France. Ce choix serait très cohérent car ce processus s’appuie sur le groupe de travail multi-acteurs lancé dans le cadre de l’Appel de Paris, dont les travaux vont reprendre en tenant compte des progrès récents.

**1/ Structurer le processus de Pall Mall dans le cadre de l’Appel de Paris**

Les réunions intermédiaires du processus de Pall Mall pourraient être convoquées dans le cadre de l’Appel de Paris et en lien avec un groupe de travail dédié au périmètre revu – à l’exception des séquences exclusivement intergouvernementales. Une telle organisation (a) permettrait d’assurer la continuité du processus en se fondant sur une initiative reconnue et ayant prouvé l’efficacité de la méthode multi-acteurs (b) tout en bénéficiant de l’expérience événementielle du Forum pour l’organisation de la réunion plénière accueillie par la France dans un an.

1. ***From a process to a success*: faire levier sur l’Appel de Paris pour la réussite de Pall Mall**

Alors que la prolifération des sommets, processus et initiatives internationales est de plus en plus pointé par l’ensemble des parties prenantes, dont les Etats, comme une menace en soi pour l'efficacité des efforts déployés pour garantir stabilité du cyberespace, le succès du processus de Pall Mall tiendra pour beaucoup à sa capacité à formuler des propositions normatives concrètes au cours d’un processus soutenu par un ordre du jour précis, tendu vers l’objectif politique fixé. L’Appel offre à ce titre un cadre de travail déjà identifié, soutenu par un secrétariat permanent expérimenté dans l’organisation du travail en format multi-acteurs et agrégeant d’ores et déjà les principaux acteurs de la société civile et du secteur privé actifs dans ce débat. Structurer les réunions intermédiaires dans le cadre de l’Appel de Paris pour sa partie multi-acteurs, et en lien avec cette communauté pour la séquence gouvernementale, permettrait de maintenir un momentum politique continu entre les deux réunions plénières en favorisant la progression des discussions substantielles.

1. **Le Forum, point d’atterrissage de la réunion 2025 du processus de Pall Mall**

L’édition annuelle 2023 du Forum a permis l’organisation d’une séquence importante sur la prolifération dans le cyberespace qui fut une étape fondatrice avant le lancement du processus de Pall Mall. Dans la prolongation des efforts conduits tout au long de l’année 2024 dans le cadre du groupe de travail de l’Appel de Paris consacré à la non-prolifération et alors que la France doit accueillir la prochaine réunion plénière du processus de Pall Mall, le Forum serait un point d’atterrissage naturel potentiellement en colocalisation avec le sommet IA pour lequel son implication est d’ores et déjà acté.

**2/ Mobiliser la communauté de l’Appel de Paris pour nourrir les discussions gouvernementales du processus de Pall Mall**

Alors que le processus de Pall Mall arrive en déclination du 5e principe de l’Appel de Paris et que la communauté multi-acteur de l’Appel s’est mobilisée sur ce sujet tout au long de 2023, il parait opportun de poursuivre une dynamique d’intégration qui permette (a) de nourrir les discussions intergouvernementales de propositions concrètes, formulées plus librement que dans un format de négociation traditionnel et (b) afin d’augmenter, via le Forum et les soutiens pertinents, la pression sur les acteurs les moins alignés avec l’initiative.

1. **Nourrir les discussions intergouvernementales de propositions émanant de la communauté des parties prenantes**

Le Forum entend poursuivre le travail initié en 2023 dans le cadre du groupe de travail de l’Appel de Paris sur les cyber-mercenaires. Le groupe de travail a notamment pour ambition 1/ de renforcer notre compréhension commune d’un phénomène complexe en rassemblant les données, analyses et études d’une communauté et 2/ de fournir des propositions concrètes visant à l’édiction d’un code de conduite pour la non-prolifération des capacités cyber sur le marché commercial, dans la continuité de la [feuille de route publiée en Novembre 2023](https://parispeaceforum.org/fr/publications/appel-de-paris-endiguer-le-marche-des-cyber-mercenaires/).

Ce travail pourra notamment compter sur un réseau d’organisations partenaires de la société civile et du secteur privé dont les capacités en matière de détection et d’analyse de ce type de menace et de ses implications sont largement reconnues. Il par ailleurs conduira à identifier des principes clairs pour la conduite du secteur privé, en particulier les opérateurs proposant des capacités d’intrusion cyber ou des prestations qui y recourent et les entreprises commercialisant les services et périphériques cibles, ainsi qu’un cadre de contrôle de telles activités par la société civile qui puisse permettre de rationaliser et mutualiser les efforts existant au sein de cette dernière – compléments indispensables aux règles de bon comportement des Etats.

1. **Renforcer la sensibilisation et le dialogue avec les écosystèmes antagonistes**

Afin d’œuvrer à l’universalisation et la bonne mise en œuvre des principes existant et à venir pour lutter contre la prolifération et l’usage irresponsable des capacités d’intrusion cyber, le Forum concentrera en priorité ses efforts de sensibilisation et sur les acteurs et contextes réfractaires :

* Dans une démarche s’inspirant des méthodes éprouvées du domaine « Security sector governance and reform », une attention particulière sera placée sur le dialogue avec les acteurs de la sécurité publique et privée, premiers utilisateurs des capacités d’intrusion cyber, autour du caractère « responsable » de l’usage de tels outils. Une série d’ateliers ciblés pourrait être organisée au cours de l’année, dont les résultats viendraient alimenter le travail normatif entrepris sur cette notion.
* Le Forum s’emploiera également à mobiliser un ensemble d’acteurs pertinents au sein des États notoirement connus comme étant des environnements favorables au développement irresponsable de capacités d’intrusion cyber et à la commercialisation de prestations afférentes, ainsi qu’au sein de ceux où un usage massif et irresponsable de telles capacités a été largement documenté. En l’absence prévisible de coopération de la part des administrations de ces États, les efforts de sensibilisation se concentreront en priorité sur les parlementaires, les relais d’opinion et les organisations clé de la société civile.