Cultures & Conflits

102 (été 2016)
Questions de méthodes

Benoît Dupont

La gouvernance polycentrique du cybercrime : les réseaux fragmentés de la coopération internationale

Avertissement
Le contenu de ce site relève de la législation française sur la propriété intellectuelle et est la propriété exclusive de l'éditeur.
Les œuvres figurant sur ce site peuvent être consultées et reproduites sur un support papier ou numérique sous réserve qu'elles soient strictement réservées à un usage soit personnel, soit scientifique ou pédagogique excluant toute exploitation commerciale. La reproduction devra obligatoirement mentionner l'éditeur, le nom de la revue, l'auteur et la référence du document.
Toute autre reproduction est interdite sauf accord préalable de l'éditeur, en dehors des cas prévus par la législation en vigueur en France.

revues.org

Revues.org est un portail de revues en sciences humaines et sociales développé par le Cléo, Centre pour l'édition électronique ouverte (CNRS, EHESS, UP, UAPV).

Référence électronique
Benoît Dupont, « La gouvernance polycentrique du cybercrime : les réseaux fragmentés de la coopération internationale », *Cultures & Conflits* [En ligne], 102 | été 2016, mis en ligne le 08 août 2018, consulté le 01 septembre 2016. URL : http://conflits.revues.org/19292

Éditeur : Centre d'études sur les conflits
http://conflits.revues.org
http://www.revues.org

Document accessible en ligne sur : http://conflits.revues.org/19292
Ce document est le fac-similé de l'édition papier.

Cet article a été téléchargé sur le portail Cairn (http://www.cairn.info).

CAIRN
Chercher. Repérer. Avancer.

Distribution électronique Cairn pour Centre d'études sur les conflits et pour Revues.org (Centre pour l'édition électronique ouverte)
Creative Commons License

La gouvernance polycentrique du cybercrime : les réseaux fragmentés de la coopération internationale

Benoît DUPONT

Benoît Dupont est professeur de criminologie à l'Université de Montréal et titulaire de la Chaire de recherche du Canada en cybersécurité. Depuis 2014, il assure la direction scientifique du Réseau intégré sur la cybersécurité (SERENE-RISC), un des réseaux de centres d'excellence (RCE) canadiens. Ses travaux portent sur les politiques publiques de sécurité et la coévolution de la délinquance et de la technologie. Il a notamment publié, avec Jennifer Wood, Democracy, society and the governance of security *(Cambridge University Press, 2006), avec Maurice Cusson et Frédéric Lemieux,* Traité de sécurité intérieure *(HMH Hurtubise, 2007), et avec Samuel Tanner,* Maintenir la paix dans les zones postconflit *(Presses de l'Université de Montréal, 2012).*

L'une des caractéristiques fondamentales de la délinquance numérique (ou du cybercrime, pour reprendre la terminologie plus fréquemment employée par les médias de masse) est sa nature transnationale, qui se manifeste par l'interaction automatisée et à une échelle sans précédent de délinquants et de victimes qui résident respectivement à des milliers de kilomètres les uns des autres. Par contraste avec cette capacité d'innovation criminelle exploitant au même rythme que les *startups* de la Silicon Valley les nouvelles technologies de l'information et de la communication, les institutions policières et judiciaires semblent avoir beaucoup plus de difficultés à s'adapter aux changements induits par un environnement numérique en constante mutation. Deux obstacles majeurs sont couramment invoqués pour expliquer cette impuissance. Le premier relève de la complexité technique associée à ce phénomène, qui constitue en soi un obstacle à son contrôle par des organisations policières issues de la Révolution industrielle et conçues pour prendre en charge des crimes à faible volume mais à fort impact (les crimes de violence), alors que la configuration actuelle des crimes numériques se caractérise au contraire par de forts volumes mais un faible impact individuel. Afin d'illus-

trer la complexité de ces nouveaux projets criminels, on citera l'exemple de la centaine d'arrestations menées en mai 2014 dans seize pays dans le but de démanteler le *botnet* BlackShades [1]. Ce réseau d'ordinateurs compromis à l'insu de leur propriétaires légitimes contrôlait environ un demi-million de machines infectées provenant d'une centaine de pays, et donc autant de victimes individuelles. Une seconde explication fréquemment avancée met l'accent sur le déficit d'harmonisation des législations nationales face à un phénomène mondialisé et sur le déficit de coordination des ressources policières qui en résulterait à l'échelle internationale. Les nombreuses politiques de cybersécurité adoptées ces dernières années par la majorité des pays occidentaux [2], ainsi que les communiqués émis à l'issue des grands sommets internationaux consacrés à cette question ont systématiquement appelé à la création et au renforcement des mécanismes de coopération opérationnelle et d'échange de renseignements.

Pourtant, un rapide recensement des initiatives de coopération mises en œuvre au cours des deux dernières décennies afin de combattre la cybercriminalité révèle une réalité bien différente, où l'on voit proliférer des réseaux hybrides mêlant services de police nationaux, organisations internationales, acteurs non gouvernementaux, associations professionnelles et entreprises. Ces nouveaux assemblages de la coopération viennent non seulement démentir l'hypothèse d'un déficit d'adaptation, mais introduisent également des configurations collaboratives assez inusitées dans le domaine du *policing* international. Afin de cartographier cette évolution et d'en caractériser les propriétés, nous mobiliserons la méthodologie de l'Analyse des réseaux sociaux (ARS), qui a fait l'objet d'applications aussi bien dans les sciences sociales [3] qu'en physique, en biologie ou encore en épidémiologie [4]. Récemment introduite dans les études criminologiques [5], cette méthode de recherche n'a cependant encore jamais été utilisée – à notre connaissance – pour analyser la structure des pratiques de coopération policière internationale. Les travaux dans ce domaine ont en effet priorisé le recours aux documents d'archives [6], aux textes juridiques [7], à des entrevues avec les acteurs

1. Europol, « Worlwide operation against cybercriminals », Communiqué de presse, 19 mai 2014, accessible en ligne : https://www.europol.europa.eu/content/worldwide-operation-against-cybercriminals (consulté le 8 juillet 2016).
2. Dupont B., « The proliferation of cyber security strategies and their implications for privacy », in Benyekhlef K. et Mitjans E. (dir.), *Circulation internationale de l'information et sécurité*, Montréal, Les Éditions Thémis, 2013, pp. 67-80.
3. Berry F., Brower R., Choi S., Xinfang Goa W., Jang H., Kwon M., et Word J., « Three traditions of network research: What the public management research agenda can learn from other research communities », *Public Administration Review*, vol. 64, n° 5, 2004, pp. 539-552.
4. Watts D., *Six degrees: The science of a connected age*, New York, W. W. Norton & Company, 2003.
5. Morselli C. (dir.), *Crime and networks*, New York, Routledge, 2014.
6. Deflem M., *Policing world society: historical foundations of international police cooperation*, New York, Oxford University Press, 2002.
7. Sabatier M., *La cooperation policière européenne*, Paris, L'Harmattan, 2011 ; Hufnagel S., *Policing cooperation across borders: Comparative perspectives on law enforcement within the EU and Australia*, Farnham, Ashgate, 2013.

clés [8], ou encore à l'ethnographie des pratiques d'échanges de renseignement [9]. En complément à toutes ces démarches méthodologiques, l'approche de l'ARS nous semble plus particulièrement fertile pour analyser à très grande échelle les diverses capacités et stratégies mobilisées par une pluralité d'acteurs, en nous donnant la possibilité de mesurer et de visualiser la multitude de liens de coopération que tissent entre eux ces acteurs de la lutte contre la cybercriminalité. Si les résultats obtenus sont essentiellement de nature quantitative, et souffrent de ce fait des inévitables biais et distorsions introduits par toute tentative de mettre en chiffre des phénomènes sociaux d'une grande complexité [10], ils révèlent néanmoins des tendances, des régularités et des déviations qui pourront ensuite amorcer et guider des questionnements qualitatifs plus poussés.

Dans le domaine de la coopération policière internationale contre la cybercriminalité, les résultats de l'analyse de réseaux semblent ainsi annoncer une transformation du *policing* international vers un mode de gouvernance polycentrique structuré autour de deux axes : un axe géographique et un axe fonctionnel. Cette articulation nouvelle constitue un quatrième modèle organisationnel de la coopération policière (après le modèle privatisé, le modèle bureaucratique et le modèle hégémonique) soulevant de nombreuses questions quant aux modalités, à la qualité et à l'imputabilité des instruments de gouvernance ainsi mis en œuvre. Cet article s'organise en quatre parties : après avoir rappelé la chronologie et les principales propriétés de chacun des trois modèles « historiques » de la coopération policière, et annoncé les raisons qui nous poussent à envisager l'émergence d'un quatrième modèle pluraliste à l'architecture distribuée, nous présenterons dans une deuxième partie les données et la méthodologie mobilisées afin de vérifier le bien-fondé de cette hypothèse. Enfin, on présentera dans une troisième et une quatrième partie les résultats obtenus par l'analyse de réseau sur les deux dimensions complémentaires de la pluralisation et du polycentrisme de la coopération, ce qui nous permettra de réfléchir aux propriétés des nouvelles structures de gouvernance qui se mettent en place à l'échelle internationale pour combattre la cybercriminalité. L'utilisation que l'on peut faire des données et des résultats ainsi obtenus sera discutée dans la conclusion.

8 . Bigo D., *Polices en réseaux : L'expérience européenne*, Paris, Presses de Sciences Po, 1996 ; Scherrer A., *G8 against transnational organized crime*, Farham, Ashgate, 2009.

9 . Sheptycki J., *En quête de police transnationale : Vers une sociologie de la surveillance à l'ère de la globalisation*, Bruxelles, Larcier, 2005.

10. Desrosières A., *La politique des grands nombres : Histoire de la raison statistique*, Paris, La Découverte, 1993 ; Porter T., *Trust in numbers: The pursuit of objectivity in science and public life*, Princeton, Princeton University Press, 1995.

Les modalités historiques de la coopération policière internationale

La coopération policière internationale est le fruit de la coévolution à un moment spécifique de formes particulières de délinquance (ou de problèmes sociaux criminalisés) faisant abstraction des frontières administratives d'un ou de plusieurs pays, d'une part, et des capacités institutionnelles et techniques des États pour prendre collectivement en charge ces phénomènes de manière adéquate, d'autre part. L'internet-centrisme ambiant voit dans l'avènement et la démocratisation des réseaux informatiques une rupture économique, politique et sociale unique dans l'histoire de l'humanité [11], ayant notamment permis l'éclosion de pratiques délinquantes automatisées se déployant à l'échelle planétaire et nécessitant donc des réponses tout aussi mondialisées. Pourtant, un simple rappel des enseignements de la littérature sur la coopération policière illustre à quel point ce discours sur l'émergence de nouveaux risques criminels transnationaux se manifeste de manière récurrente depuis la seconde moitié du XIXe siècle, de concert avec la mise en place de régimes de prohibition successifs [12].

Privatisation

Dès la Révolution industrielle, l'expansion du commerce international et des investissements de grandes firmes européennes et américaines à l'étranger a généré pour ces dernières des besoins nouveaux en matière de protection de leurs intérêts commerciaux et financiers. L'absence à cette époque de structures formelles d'échange d'informations policières à l'échelle internationale favorise alors le développement d'initiatives privées accessibles aux clients fortunés et aux empires industriels en construction, dont la mieux documentée reste certainement l'agence Pinkerton, qui cultivait de précieux contacts parmi les chefs de police des grandes métropoles européennes et dont la traque de Butch Cassidy en Argentine et en Bolivie est l'un des éléments les moins connus de la saga du *Sundance Kid* [13]. La Banque d'Angleterre fit appel aux services de Pinkerton dans les années 1870 pour une affaire de fraude, donnant lieu à l'une des premières enquêtes internationales dans ce domaine, et l'enlèvement d'un fugitif américain au Pérou par un détective de l'agence en exécution d'un mandat d'arrestation du gouvernement fédéral donna lieu en 1886 au premier jugement de la Cour suprême des États-Unis légalisant de telles pratiques d'extraditions extraordinaires [14]. Ce modèle privatisé de coopéra-

11. Morozov E., *Pour tout résoudre, cliquez ici ! L'aberration du solutionnisme technologique*, Paris, Fyp Éditions, 2014.
12. Anderson M., *Policing the world: Interpol and the politics of international police co-operation*, Oxford, Clarendon Press, 1989 ; Deflem M., *op. cit.* ; Andreas P. et Nadelmann E., *Policing the globe: Criminalization and crime control in international relations*, Oxford, Oxford University Press, 2006.
13. Morn F., *The eye that never sleeps: A history of the Pinkerton national detective agency*, Bloomington, Indiana University Press, 1982.
14. Andreas P. et Nadelmann E., *op. cit.*

tion ne résista pas à l'affirmation par les États de leur souveraineté juridique et territoriale, mais loin d'avoir totalement disparu, il s'incarne aujourd'hui dans l'industrie florissante des consultants transnationaux en sécurité et en gestion des risques. Ceux-ci fournissent aux entreprises et aux gouvernements ne disposant pas de telles ressources l'accès à de véritables réseaux privés de renseignement, leur permettant de retracer les comptes dissimulés de dictateurs déchus ou de négocier la rançon et la libération sans effusion de sang de personnels kidnappés [15]. Les États ont également recours à cette modalité de la coopération policière lorsqu'ils souhaitent soustraire certaines de leurs opérations aux contrôles juridiques et administratifs normalement prévus dans un tel contexte, et ainsi conserver une capacité de dénégation plausible en cas de scandale médiatique.

Bureaucratisation

L'émergence des bureaucraties policières, la professionnalisation des services d'enquête et l'intensification des échanges internationaux au début du XXe siècle donnèrent progressivement naissance à des structures administratives de coopération qui se substituèrent aux mécanismes informels d'échange de renseignement, en Europe d'abord, puis en Amérique du Nord. Dans l'historiographie officielle d'Interpol, c'est certainement le premier Congrès de police judiciaire internationale, tenu à Monaco en 1914 [16], qui marqua le basculement vers l'idée d'une structure supranationale permettant de systématiser les pratiques de coopération. Brutalement interrompu par la Première Guerre mondiale, ce processus d'internationalisation bureaucratique fut relancé de manière décisive par la création de la Commission internationale de police criminelle (CIPC) lors du Congrès de Vienne en 1923. Basé dans cette même ville, le quartier général de la CIPC développa au cours des années qui suivirent des outils destinés à faciliter l'échange d'informations : registres des personnes recherchées ou jugées dangereuses par les services de police des pays membres, listes de passeports contrefaits, fichiers contenant les empreintes digitales et les photographies des délinquants internationaux, système codé de communication télégraphique traduit en six langues, réseau radio international, dictionnaire des enquêtes criminelles, bottin international des organisations policières ou autres mensuels consacrés à la diffusion de statistiques criminelles contribuèrent à la création de canaux de communication facilitant la circulation des renseignements [17].

15. O'Reilly C. et Ellison G., « Eye spy private high: Re-conceptualizing high policing theory », *The British Journal of Criminology*, vol. 46, n° 4, 2006, pp. 641-660 ; O'Reilly C., « L'évolution de l'offre des professionnels du risque mondialisé », *Champ Pénal – Penal Field*, vol. X, 2013, accessible en ligne : https://champpenal.revues.org/8611 (consulté le 8 juillet 2016).
16. On pourra en consulter le programme intégral, comprenant aussi bien la liste des thèmes et intervenants que les suggestions sur les hôtels recommandés ou les excursions proposées en marge du congrès, sur Gallica, la plateforme numérique de la Bibliothèque nationale de France : http://gallica.bnf.fr/ark:/12148/bpt6k5690823p (consulté le 8 juillet 2016).

La focalisation de ce modèle de coopération sur les dimensions purement techniques et administratives ne découle pas exclusivement d'un souci d'efficacité propre à tout phénomène de professionnalisation, mais aussi de la volonté de projeter, dans une période où l'Europe restait encore traversée de tensions belliqueuses et s'apprêtait à replonger dans un conflit mondial, une image d'autonomie organisationnelle permettant de surmonter les réticences diplomatiques d'anciens ennemis [18]. Si l'organisation qui donnera naissance à Interpol passa durant les années 1940 sous contrôle nazi, avant d'être exposée aux tentatives d'instrumentalisation des deux grandes puissances au cœur de la guerre froide pendant les années 1950 et 1960 [19], l'idéal d'une organisation internationale modelée sur le modèle wébérien d'une expertise indépendante des pouvoirs politiques nationaux demeura intact. Cela explique également en grande partie pourquoi Interpol se focalisa sur la délinquance de droit commun et se récusa des crimes à connotation politique. Cette autonomisation de la coopération par la bureaucratisation prit de surcroît le parti de ne jamais pousser la logique à son terme, jusqu'à la compétition directe avec les organisations policières nationales. Le respect strict de la souveraineté des États, exprimé par la création dans chaque pays d'un Bureau central national (BCN) composé de policiers locaux conservant le contrôle des flux d'informations entrantes et sortantes, vint ainsi garantir que les membres n'eurent jamais à se sentir menacés par les activités d'Interpol et continuèrent de lui offrir leur soutien.

Une rationalité similaire de bureaucratisation fut à l'œuvre dans la création d'Europol en 1992, même si la démarche par le haut adoptée selon une procédure accélérée par les institutions européennes et la crainte d'un processus de fédéralisation policière donnèrent lieu à des réticences initiales [20]. Celles-ci furent apaisées par la limitation de son mandat à des activités d'échange de renseignement. Plus récemment, la transformation en 2009 d'Europol en agence européenne, ainsi que son implication de plus en plus fréquente dans des activités opérationnelles menées conjointement avec des forces de police nationales européennes, mais également nord-américaines, laisse supposer que l'autonomisation bureaucratique n'est pas totalement incompatible avec des reconfigurations de souveraineté.

La logique de bureaucratisation et de « verticalisation » de la coopération décrite ici n'est pas uniquement d'ordre institutionnel, puisqu'elle transforme également en profondeur les pratiques professionnelles, favorisant l'apparition de nouveaux profils d'expertise incarnés par les agents de liaison ou les experts chargés de produire et de diffuser les normes émergentes en matière de lutte contre la délinquance transnationale [21]. Disposant d'un important

17. Deflem M., *op. cit.*, p. 124 et suiv.
18. *Idem*.
19. Anderson M., *op. cit.*, p. 45.
20. Bigo D., *op. cit.* ; Hufnagel, S., *op. cit.*

capital culturel (notamment une maîtrise avancée de la langue anglaise et une formation universitaire initiale dans le domaine de la géopolitique ou du droit international) et provenant d'organisations nationales prestigieuses (diplomatie, justice, intérieur) impliquées dans les négociations internationales, ces nouveaux professionnels de la coopération aux trajectoires diversifiées valorisent les compétences analytiques permettant de traiter les volumes exponentiels d'informations dont ils doivent assurer la fluidité transfrontalière, ce qui les distingue d'une culture policière opérationnelle plutôt vouée à l'action. Leur rôle de courtier entre des institutions aux rationalités organisationnelles et aux capacités très diversifiées leur confère également un fort capital social et une reconnaissance indéniable au sein de leur organisation d'origine, que les plus ambitieux convertissent ensuite en promotions accélérées. Scherrer a également mis en lumière la solidarité professionnelle que développent ces acteurs à l'intersection des institutions nationales et internationales, qui contribue à l'émergence d'une compréhension commune des problèmes de sécurité et des stratégies de coopération devant être mises en œuvre pour y répondre, et permet ainsi de surmonter les querelles internes à travers un consensus *a minima* [22].

Hégémonisme

Le processus de bureaucratisation décrit dans la section précédente ne produit pas uniquement des capacités nouvelles en matière de coopération. Il contribue également à l'émergence de contraintes procédurales additionnelles dont la pesanteur peut alimenter le cynisme des acteurs de terrain. Par ailleurs, le déficit structurel de cohésion et d'harmonisation des capacités et des pratiques au sein d'une organisation telle qu'Interpol, qui compte près de 200 membres internationaux, se traduit concrètement par une difficulté chronique à mobiliser efficacement sur des problèmes criminels ne faisant pas consensus. Ces contreparties inévitables à l'émergence de bureaucraties babéliennes génèrent des frustrations non négligeables parmi les pays engagés dans des campagnes de répression agressives. Lorsque ceux-ci disposent par ailleurs de ressources économiques et politiques suffisantes, la tentation de s'émanciper de la pesanteur des structures bureaucratiques existantes et de mettre en place des dispositifs *ad hoc* de coopération policière, exonérés de toute nécessité de compromis, devient alors irrésistible.

21. Bigo D., *op. cit.*, p. 27 et suiv. ; Scherrer A., *op. cit.* ; den Boer M., « Towards a governance model of police cooperation in Europe: The twist between networks and bureaucracies », in Lemieux F. (dir.), *International police coopération: Emerging issues, theory and practice*, Cullompton, Willan, 2010, pp. 57-58 ; Stalcup M., « Interpol and the emergence of global policing », in Garriott W. (dir.), *Policing and contemporary governance: The anthropology of police in practice*, New York, Palgrave MacMillan, p. 240.
22. Scherrer A., *op. cit.*, p. 57 et suiv. ; Scherrer A. et Dupont B., « Nœuds ou champs ? Analyse de l'expertise internationale sur la criminalité transnationale organisée et le terrorisme », *La Revue Canadienne de Criminologie et de Justice Pénale*, vol. 52, n° 2, 2010, pp. 147-172.

Si le modèle bureaucratique a vu le jour sur le continent européen, cette projection hégémonique des ressources policières sur la scène internationale a d'abord été mise en œuvre par les États Unis. Dans le contexte de la mise en place d'un régime mondial de prohibition accélérée par la Guerre contre la drogue déclarée par le Président Nixon au début des années 1970 [23], les agences de police fédérale américaines déploient depuis une cinquantaine d'années des ressources considérables réparties à l'échelle planétaire afin de perturber les flux transnationaux de stupéfiants. Ethan Nadelmann a ainsi très clairement montré comment la *Drug Enforcement Agency* avait établi un réseau tentaculaire d'agents de liaison ayant facilité l'adoption par les services de police européens de méthodes et de techniques d'enquêtes calquées sur les priorités américaines. Une stratégie identique fut utilisée en Amérique latine afin de renforcer les capacités locales et tenter de neutraliser les filières de production, de trafic et de blanchiment, tout ceci dans un environnement politique local où la corruption était routinière [24]. En 1994, les États Unis disposaient ainsi de plus de 2 000 agents fédéraux d'application de la loi (principalement FBI et DEA) détachés dans leurs représentations diplomatiques à l'étranger, chiffre ne tenant évidemment pas compte des agents de renseignement dont le nombre s'est probablement considérablement accru après les attentats du 11 septembre [25]. Par contraste, on rappellera qu'Interpol employait à peine plus de 750 personnes en 2013 [26]. Bien que ce modèle implique de nombreux partenariats bilatéraux forgés au gré des besoins et des reconfigurations des risques transnationaux, le déséquilibre des moyens en présence reflète bien plus une logique de domination que de véritable coopération.

Polycentrisme

Les trois modèles de coopération esquissés plus haut sont présentés de manière chronologique afin d'en faciliter l'examen, mais ils ne doivent pas être envisagés sur le mode de la substitution ou du remplacement historique, bien au contraire. Leur coexistence contemporaine reflète plutôt une logique d'empilement et d'interconnexion produisant des assemblages hybrides de sécurité. Ce polycentrisme reflète la nouvelle « architecture du *policing* globalisé », où des organisations policières internationales, des agences de police régionales, des pôles nationaux intégrés d'enquête, des acteurs privés de la sécurité transnationale, ainsi que des structures policières locales sont enchâssés dans un réseau mondial de collaborations et d'interdépendances [27]. L'analyse théorique de ce pluralisme institutionnel et de ses mécanismes de coordination

23. Gregory F., « Private criminality as a matter of international concern », in Sheptycki J. (dir.), *Issues in transnational policing*, Londres, Routledge, 2000, p. 111 ; Andreas P. et Nadelmann E., *op. cit.*, p. 37 et suiv.
24. Nadelmann E., *Cops across borders: The internationalization of U.S. criminal law enforcement*, University Park, The Pensylvannia State University Press, 1993, pp. 189-312.
25. Bowling B. et Sheptycki J., *Global policing*, Londres, Sage, 2012, p. 48.
26. Interpol, *Rapport annuel 2013*, Lyon, Interpol, 2014, p. 9.

peut bien évidemment donner lieu à des interprétations divergentes [28], mais on se concentrera dans cet article sur le concept de réseau de sécurité, inspiré des travaux de Shearing et de ses collègues sur la gouvernance nodale et de leur analyse des divers *nodes* ou nœuds institutionnels qui déploient des technologies, des mentalités et des ressources diversifiées afin de peser sur le cours des évènements [29].

Ces *nodes* institutionnels, loin d'agir de manière isolée, sont enchâssés dans des réseaux de politiques publiques dont les outils méthodologiques d'analyse des réseaux sociaux nous aident à comprendre la nature et la structure. Nous définissons par conséquent un réseau de sécurité comme « un groupe d'acteurs institutionnels, organisationnels, communautaires ou individuels interconnectés dans le but de mandater ou de produire des activités de mise en sécurité au bénéfice de parties prenantes, internes ou externes » [30]. La notion de réseau de sécurité permet d'appréhender de manière globale les nouvelles configurations qui transforment les institutions policières et leur travail, ainsi que le pluralisme des modes d'accès à la sécurité, soit comme bien public ou au contraire comme produit d'une activité commerciale. En d'autres termes, cette approche permet d'étudier simultanément les processus de privatisation, de bureaucratisation et d'hégémonie à l'œuvre en matière de lutte contre la cybercriminalité, plutôt que de se cantonner à une analyse chronologique par définition réductrice, et de montrer sur la base de données empiriques comment ces dispositifs *a priori* antinomiques s'intègrent les uns aux autres. Cette approche a également l'avantage d'envisager la sécurité non seulement comme le résultat de l'activité spécifique de chaque organisme disposant d'un mandat dans ce domaine, mais aussi comme le produit des nombreuses interactions et interdépendances qui lient ces organismes. Autrement dit, la vision « émergente » qui en découle relève de l'idée aristotélicienne classique selon laquelle un tout est plus grand que la somme de ses parties : le tout étant ici la sécurité, les parties les institutions publiques et privées assumant des responsabilités afférentes dans ce domaine, et les propriétés émergentes relevant de la valeur ajoutée produite par les liens de collaboration unissant ces institutions.

Par contraste avec les travaux originels sur la gouvernance nodale, qui exploitent principalement la dimension métaphorique associée à la notion de réseau, les recherches sur les réseaux de sécurité reposent sur la collecte systématique de données quantitatives et qualitatives permettant d'identifier et d'analyser les propriétés des configurations polycentriques de production de

27. Bowling B. et Sheptycki J., *op. cit.*, p. 53 ; Wall D., « Policing cybercrimes: Situating the public police in networks of security within cyberspace », *Police Practice and Research: An International Journal*, vol. 8, n° 2, 2007, pp. 183-205.
28. Scherrer A., Dupont B., *op. cit.*
29. Drahos P., Shearing C., Burris S., « Nodal governance as an approach to regulation », *Australian Journal of Legal Philosophy*, vol. 30, 2005, pp. 30-58.
30. Dupont B., « Security in the age of networks », *Policing and Society*, vol. 14, n° 1, 2004, p. 78.

la sécurité. Initialement développée pour étudier le fonctionnement de réseaux locaux de sécurité urbaine [31], cette approche a ensuite été utilisée dans les contextes de la sécurité portuaire [32], de l'anti-terrorisme [33], du *policing* des grands événements sportifs [34], ou encore du contrôle de certaines formes de délinquance en ligne telles que le piratage de produits culturels ou encore le cyber-harcèlement [35]. Dans le prolongement de ces recherches, cet article constitue à notre connaissance la première tentative d'application à des initiatives de coopération policière internationale.

L'analyse des réseaux sociaux

La démarche empirique suivie dans cet article s'inscrit dans la tradition de l'ARS. Celle-ci connaît depuis quelques années un développement accéléré parmi les disciplines relevant des sciences sociales, notamment du fait de la disponibilité accrue de logiciels d'analyse et de visualisation relativement aisés d'utilisation (Ucinet, Gephi, NodeXL, Pajek, R, NetMiner, pour ne citer que les plus connus), ainsi que de la simplicité déconcertante avec laquelle les outils informatiques existant permettent la constitution de bases de données relationnelles à partir des nombreuses traces laissées par les activités et les interactions des usagers sur internet [36]. L'ARS précède cependant l'avènement de l'informatique et de l'Internet de plusieurs décennies, puisqu'elle tire son origine des travaux menés par Jacob Moreno sur la sociométrie dès les années 1930 [37]. La finalité de cette méthodologie est de permettre « une analyse structurale dont le but est de montrer en quoi la forme du réseau a une incidence sur les phénomènes analysés, tout en étant le résultat des interactions qui y ont cours » [38]. Les relations entre acteurs y prennent donc une place déterminante, par contraste avec des approches sociologiques plus classiques qui se préoccupent plutôt des attributs individuels (âge, revenus, genre, etc.) permettant de constituer des catégories homogènes. Cette distinction fondatrice qui permet

31. Jones T., Newburn T., *Private security and public policing*, Oxford, Oxford University Press, 1998 ; Dupont B., « Delivering security through networks: Surveying the relational landscape of security managers in an urban setting », *Crime, Law and Social Change*, vol. 45, n° 3, 2006, pp. 165-184.
32. Brewer R., *Policing the waterfront: Networks, partnerships, and the governance of port security*, Oxford, Oxford University Press, 2014.
33. Whelan C., *Networks and national security: Dynamics, effectiveness and organisation*, Londres, Ashgate, 2012.
34. Whelan C., « Surveillance, security and sporting mega events: Toward a research agenda on the organisation of security networks », *Surveillance & Society*, vol. 11, n° 4, 2014, pp. 392-404.
35. Nhan J., Huey L., « Policing through nodes, clusters and bandwith », in Leman-Langlois S. (dir.), *Technocrime: Technology, crime and social control*, Cullompton, Willan, 2008, pp. 66-87 ; Broll R., « Collaborative responses to cyberbullying: Preventing and responding to cyberbullying through nodes and clusters », *Policing and Society*, DOI : 10.1080/10439463.2014.989154, sous presse, pp. 1-18.
36. Watts D., « The "new" science of networks », *Annual Review of Sociology*, vol. 30, 2004, p. 243.
37. Freeman L., *The development of social network analysis: A study in the sociology of science*, Vancouver, Empirical Press, 2004, pp. 31-42.
38. Degenne A., Forsé M., *Les réseaux sociaux*, Paris, Armand Colin, 2004, p. 8.

de mieux saisir la contribution originale de l'analyse des réseaux à la compréhension des phénomènes sociaux s'efface progressivement, puisque de nouvelles approches statistiques combinent l'étude des données relationnelles avec celle des attributs catégoriels [39].

Concrètement, les données relationnelles sont formellement représentées grâce à des outils mathématiques et algébriques relevant de la théorie des graphes [40]. Ceux-ci permettent de représenter les acteurs d'un réseau (les sommets en langage des graphes), les liens qui les unissent (les arêtes), et de mesurer les propriétés structurelles des réseaux sociaux étudiés, telles que la densité ou la centralisation [41]. Dans le cas qui nous occupe, le réseau n'est pas constitué d'individus mais plutôt d'organisations qui maintiennent des liens formels de coopération. Si ce réseau composé de membres institutionnels fonctionne de manière très différente des groupes plus restreints d'individus habituellement étudiés par les sociologues ou les anthropologues, les méthodes algébriques applicables demeurent les mêmes.

Notre réseau se distingue enfin par le fait qu'il comprend deux catégories distinctes de sommets : des acteurs organisationnels, d'une part, et les initiatives de coopération auxquels ceux-ci participent, d'autre part. On parle dans ce cas de réseau d'affiliation ou de réseau à deux dimensions [42]. Cette approche spécifique permet en effet de considérer simultanément les niveaux micro et macro d'un réseau, en observant quels acteurs appartiennent (ou pas) à quelles plateformes de coopération, et d'en déduire certaines hypothèses quant aux diverses stratégies d'affiliation, d'association et d'interaction mises en œuvre, ainsi que sur les choix opérés en matière d'allocation du capital social. En d'autres termes, cette méthode permet d'analyser empiriquement l'interpénétration de réseaux d'organisations dédiées à la lutte contre la cybercriminalité et des réseaux d'initiatives de coopération qui les unissent, dans ce que Ronald Breiger définit comme l'intersection d'organisations au sein de mécanismes de coopération, et de mécanismes de coopération au sein d'organisations [43].

39. De Nooy W., Mrvar A., Batagelj V., *Exploratory social network analysis with Pajek*, 2e édition, Cambridge, Cambridge University Press, 2011, p. 27.
40. Wasserman S., Faust K., *Social network analysis: Methods and applications*, Cambridge, Cambridge University Press, 1994.
41. La densité est définie comme « la proportion des relations observées relativement aux relations possibles entre acteurs », alors que la centralisation du système « reflète la variabilité des scores individuels » de centralité de chacun des acteurs qui composent un réseau. Voir Lazega E., *Réseaux sociaux et structures relationnelles*, Paris, Presses Universitaires de France, 2007, pp. 45 et 46. Des présentations détaillées des termes techniques et des méthodes de l'analyse des réseaux sociaux sont aussi disponibles en français dans Lemieux V., Ouimet M., *L'analyse structurale des réseaux sociaux*, Québec, Les Presses de l'Université Laval, 2004 ; ou encore Degenne A., Forsé M., *op. cit.*
42. Cristofoli P., « Aux sources des grands réseaux d'interaction », *Réseaux*, n° 152, 2008, pp. 21-58.
43. Breiger R., « The duality of persons and groups », *Social Forces*, vol. 53, n° 2, 1974, pp. 181-190.

Notre corpus de données comprend 657 acteurs impliqués dans 51 initiatives internationales multilatérales de lutte contre la cybercriminalité, dont la plus ancienne a débuté ses activités en 1990 [44]. Il est à ce stade important de définir de manière plus précise ce que recouvre le terme « initiative » : dans cette étude, une initiative est un regroupement stable d'acteurs organisationnels conduisant des activités spécifiques pour lutter contre la cybercriminalité, qu'il s'agisse de campagnes de prévention, de formations destinées à divers types d'intervenants, de mécanismes de partage du renseignement, d'opérations de démantèlement de réseaux criminels, de démarches visant à harmoniser les législations nationales, etc. Ces activités concrètes doivent produire des résultats mesurables, ce qui exclut les forums de discussion se limitant à l'organisation de réunions, et doivent s'inscrire dans une durée minimale de plusieurs années. Certaines de ces initiatives opèrent ainsi de manière permanente, alors que d'autres bénéficient de budgets temporaires qui limitent leur durée de vie à quelques années. On distingue également ces initiatives selon leur origine institutionnelle : quelques-unes émanent d'organisations internationales déjà établies (comme Interpol ou l'Union internationale des télécommunications par exemple) qui se dotent ainsi de moyens d'action spécialisés, alors qu'une seconde catégorie d'entre elles sont créées *ex nihilo* par des collectifs d'acteurs tentant de répondre à un besoin commun ou de mutualiser certaines ressources spécifiques. Les données ont été recueillies au cours de l'été et de l'automne 2014 en effectuant des recherches sur les principales bases de données bibliographiques, sur les sites des grandes organisations internationales (Interpol, Europol, ONU, UE, etc.), ainsi qu'en dépouillant la littérature grise publiée par les principaux services policiers ou les grandes entreprises ayant fait de la lutte contre la cybercriminalité l'une de leurs priorités. Ces recherches nous ont permis de réunir 190 documents de portée variable allant d'un état détaillé de la coopération anti-cybercriminalité à la présentation approfondie d'une initiative particulière, de ses objectifs et de ses résultats. Chacun de ces documents fut ensuite codé afin d'extraire les données sur les initiatives identifiées et les acteurs affiliés à chacune d'entre elles. Pour chaque initiative, des informations sur le nombre de membres affiliés, l'année de création, le secteur institutionnel en assurant le pilotage (public, privé ou associatif), ainsi que les activités menées furent compilées. Afin de mener les analyses de réseau, les données d'affiliation furent enregistrées dans une matrice de coparticipation où les lignes représentent les acteurs et les colonnes les initiatives. Notre matrice complète comprend ainsi 657 lignes et 51 colonnes, ce qui permet de représenter 33 507 affiliations potentielles. La saisie des données, leur manipulation, leur analyse et la visualisation des résultats furent réalisées à l'aide du logiciel spécialisé Ucinet [45], qui met à la disposition de ses utilisateurs des outils et algorithmes créés par un grand nombre de chercheurs et permettent de calculer les principales mesures employées pour analyser et représenter la structure des réseaux sociaux.

44. La liste complète de ces 51 initiatives est présentée dans l'Annexe.

La pluralisation de la coopération internationale contre la cybercriminalité

Cinq constatations initiales peuvent être faites à la simple inspection des données recueillies. En premier lieu, et contrairement à ce que l'on peut parfois lire dans la presse généraliste ou même entendre dans certains forums professionnels, on voit proliférer depuis une trentaine d'années les initiatives de coopération internationale en matière de lutte contre la cybercriminalité. Comme nous l'avons déjà indiqué, nous en avons recensé pas moins de 51, sans prétendre à l'exhaustivité. Sans préjuger de l'efficacité de ces initiatives, force est donc de constater que le déficit des outils de coordination souvent invoqué relève d'une méconnaissance des structures existantes.

En second lieu, l'argument d'un manque d'adaptation des institutions à cette nouvelle forme de délinquance qu'est la cybercriminalité semble également ignorer la chronologie de création des initiatives de coopération : en effet, 15 % des initiatives recensées virent le jour durant les années 1990 (la première d'entre elles en 1990), 55 % durant les années 2000, et 25 % durant la première moitié des années 2010 [46]. Il semble donc évident que les efforts multilatéraux de lutte contre la cybercriminalité ont suivi de manière assez rapide la démocratisation de l'internet et l'émergence d'une délinquance en ligne mondialisée.

En troisième lieu, les mandats de ces initiatives sont relativement variés et relèvent de cinq grandes catégories d'activités, comme l'illustre le tableau 1 ci-dessous. Des efforts importants semblent consentis en matière de renforcement des capacités, en particulier pour les pays en voie de développement, alors que les activités opérationnelles demeurent encore minoritaires. À travers les activités de lobbying émanant de certaines ONG sur lesquelles on reviendra plus loin, on discerne également la place occupée par des entrepreneurs de morale dans ce réseau de coopération [47].

Activités	Pourcentage
Renforcement des capacités	74,5 %
Échange de renseignement	49,0 %
Soutien législatif et règlementaire	37,2 %
Opérations répressives (enquêtes criminelles, collecte de renseignement)	31,4 %
Lobbying	9,8 %

Tableau 1 : Types d'activités promues par les 51 initiatives

Note : le total est supérieur à 100 %, puisque certaines initiatives disposent de mandats multiples.

45. Borgatti S., Everett M., Freeman L., *Ucinet for Windows: Software for social network analysis*, Harvard, Analytic Technologies, 2002.
46. On ne dispose pas d'informations fiables sur la date de création des trois initiatives restantes.
47. Becker H., *Outsiders*, Paris, Métailié, 1985, pp. 171-187.

En quatrième lieu, l'ampleur des initiatives de lutte contre la cybercriminalité s'avère d'une grande variabilité. La participation moyenne pour les 51 initiatives analysées est de 41,2 membres (médiane de 21), avec un minimum de cinq participants pour le *Strategic alliance cyber crime working group* et un maximum de 251 participants pour le *Forum of incident response and security teams* (FIRST). Le diagramme 1 représente la distribution des initiatives selon le nombre de participants, et cette visualisation permet de rapidement identifier deux groupes distincts : le premier est constitué des initiatives ne comprenant pas plus de 50 participants, reflétant une focalisation géographique ou fonctionnelle particulière telle que l'Europe, l'Amérique latine, les pays du *Commonwealth*, le secteur privé ou des fonctions policières ou judiciaires. La seconde catégorie réunit pour sa part les membres du club beaucoup plus sélect des cinq initiatives comptant plus de 200 participants. Deux de ces initiatives sont pilotées par Interpol, deux autres par l'Union internationale des télécommunications (UIT), alors que la dernière – qui est aussi la plus importante par le nombre de membres – est une initiative émanant du secteur privé (le FIRST). En raison de la méthodologie employée, cette différence significative de taille aura des répercussions non négligeables sur les résultats des analyses, qu'il sera important de garder à l'esprit.

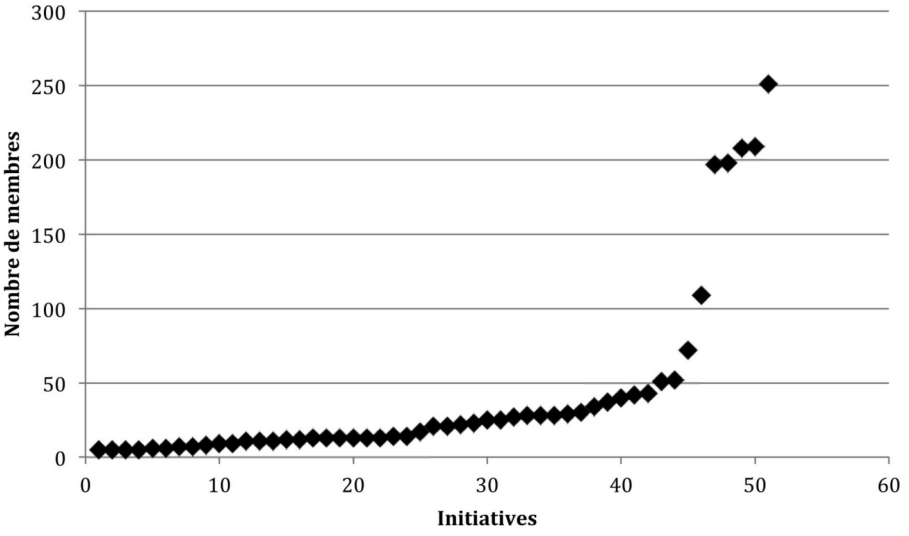

Diagramme 1 : Distribution des initiatives selon le nombre de membres

Une cinquième et dernière observation concerne le rôle déterminant joué par le secteur privé dans la lutte contre la cybercriminalité. L'analyse des organisations responsables de l'élaboration et de la mise en œuvre des 51 initiatives à l'étude place toujours les institutions gouvernementales et internationales au premier rang, avec 63 % des projets pilotés. Mais les organisations non gouvernementales et les entreprises sont loin d'être marginalisées, puisqu'elles sont respectivement à l'origine de 33 % et 12 % des initiatives analysées [48]. Le tableau 2 présente la distribution des 657 acteurs associés aux 51 initiatives selon leurs caractéristiques organisationnelles.

Type d'acteurs	Nombre	Pourcentage
Pays (organisations policières et judiciaires, de l'Afghanistan au Zimbabwe)	204	31 %
Organisations internationales (par exemple : Interpol, la Banque mondiale, l'Organisation des États américains ou la *Commonwealth telecommunications organization*)	38	6 %
ONG et associations professionnelles (par exemple : Innocence en danger, *Save the Children*, *Global prosecutors E-crimenetwork*, ou l'*International bar association*)	103	16 %
Entreprises (par exemple : Société générale, Orange, Microsoft, ou Cassidian)	312	47 %
Total	**657**	**100 %**

Tableau 2 : Types d'acteurs organisationnels participant aux 51 initiatives internationales de lutte contre la cybercriminalité

Alors que l'implication massive du secteur privé est prévisible, puisqu'il est le propriétaire et l'opérateur par défaut des infrastructures technologiques et des services affectés par les divers risques numériques, la place occupée par les ONG mérite plus d'explications. On retrouve principalement dans cette catégorie deux groupes d'acteurs : des associations de policiers, de procureurs, de juges, d'experts en sécurité informatique ou encore de chercheurs qui placent la lutte contre la cybercriminalité au cœur de leurs activités professionnelles, ainsi que des associations de protection des droits des enfants. Ces dernières, constituées principalement de citoyens et de parents concernés par la consommation de pornographie juvénile et l'exploitation sexuelle des enfants, mobilisent l'opinion publique afin de faire adopter des législations plus sévères et d'obtenir les ressources financières nécessaires à leur application. Les activités nationales de ces associations préoccupées par les effets néfastes de l'internet sur le développement des enfants ont fait l'objet de publications mettant en lumière leur contribution à l'émergence et à la propagation de

48. La somme des trois pourcentages est supérieure à 100, car certaines initiatives sont conjointement pilotées par plusieurs types d'acteurs (gouvernements et ONG par exemple).

paniques morales [49]. Toutefois, leur rôle sur la scène internationale demeure méconnu. Pourtant, pas moins de 13 des 51 initiatives recensées (25 %) relèvent de la protection de l'enfance, et incarnent des alliances stratégiques forgées par ces associations nationales de lutte contre la pédopornographie avec des multinationales des télécommunications ou du secteur bancaire et des organisations internationales. Ces ONG semblent ainsi disposer d'une influence considérable leur permettant de mobiliser les acteurs gouvernementaux et privés afin de développer des activités de coopération sur une forme de cyber-délinquance pour laquelle on ne dispose encore que de statistiques extrêmement rares et d'une fiabilité bien incertaine.

La structure polycentrique de la coopération policière : cohésion, centralité, proximité et intermédiarité

Une fois enregistrées dans la matrice de coparticipation, les données relationnelles peuvent être représentées au moyen d'un outil intégré au logiciel Ucinet qui permet à l'utilisateur de les visualiser selon les propriétés du réseau qu'il désire mettre en valeur. Dans le diagramme 2, nous utilisons un algorithme de positionnement multidimensionnel (*Multi dimensional scaling*) afin de regrouper les acteurs et les initiatives selon leur degré de similarité ou de dissemblance dans la structure des liens d'affiliation recensés. La visualisation ainsi obtenue permet d'identifier quelques nuages distincts d'acteurs et d'initiatives. Ces dernières (représentées par des carrés noirs) se répartissent en effet en deux agrégats principaux : à la gauche du diagramme sont réunies les initiatives soutenues par des institutions européennes, alors que le groupe de droite rassemble de manière plus dispersée des initiatives internationales (promues par Interpol et l'UIT) ou régionales (Asie, Amérique du Nord, ou Amérique latine par exemple). Quelques points isolés (l'*European NGO Alliance for child safety online* ou eNACSO, et la *Financial coalition against child pornography* ou FCAP), en haut et en bas du diagramme, pointent par ailleurs certaines initiatives plus autonomes et moins connectées au réseau global, probablement en raison de la nature très spécialisée de leur mandat.

49. Marwick A., « To catch a predator? The MySpace moral panic », *First Monday*, vol. 13, n° 6, 2008, accessible en ligne : http://firstmonday.org/ojs/index.php/fm/article/viewArticle/2152 (consulté le 8 juillet 2016) ; Clapton G., Cree V. et Smith M., « Moral panics and social work: Towards a sceptical view of UK child protection », *Critical Social Policy*, vol. 33, n° 2, 2013, pp. 197-217.

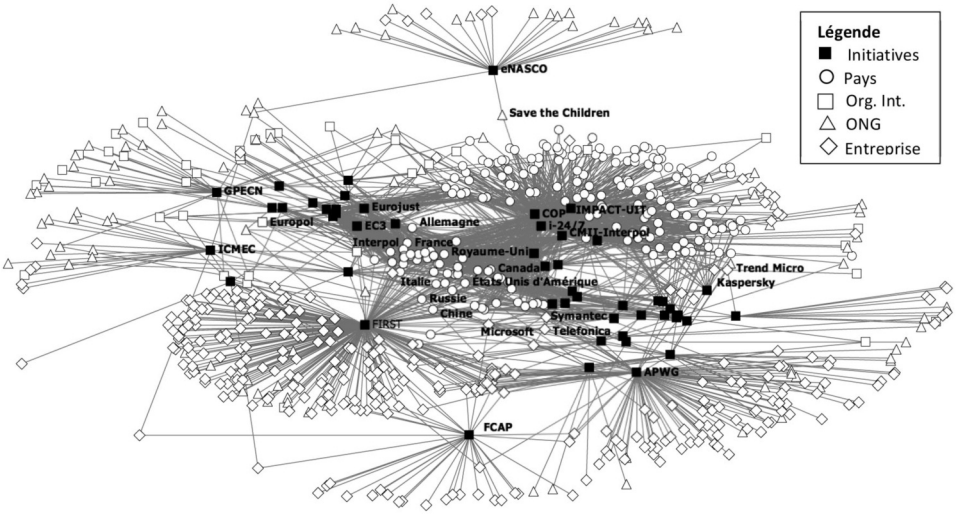

Diagramme 2 : Réseau de coopération internationale contre la cybercriminalité

On observe également que les acteurs tendent à être regroupés selon leurs caractéristiques organisationnelles, les institutions gouvernementales nationales, les entreprises et les ONG ayant tendance à se regrouper en grappes. Il est important de rappeler ici que la représentation graphique est le résultat d'une analyse des relations et non des propriétés des acteurs ou des initiatives. Ceci implique que ces regroupements expriment des modes d'affiliation en partie influencés par les caractéristiques organisationnelles des acteurs – plutôt que par des variables externes en lien avec les objectifs poursuivis. Cette affiliation influencée par les affinités ne favorise pas nécessairement la construction des partenariats les plus efficaces possibles, qui bénéficieront de la diversité des moyens et des capacités qu'ils peuvent réunir. Les initiatives développées par le secteur privé afin de coordonner à l'échelle internationale la réponse aux incidents informatiques (le FIRST) ou à la fraude bancaire en ligne (*Anti phishing working group* ou APWG) apparaissent ainsi comme bien moins attractives pour les institutions gouvernementales que celles parrainées par Interpol ou l'UIT, alors que ces dernières sont elles-mêmes inaccessibles aux entreprises qui disposent pourtant de capacités significatives pour contrôler certaines formes de cybercriminalité et garantir la sécurité de l'information de leurs usagers. Cette ségrégation n'est toutefois pas absolue, puisque certains acteurs privés disposant d'une expertise reconnue en sécurité informatique et commercialisant des produits ou des services dans ce domaine, sont positionnés à très grande proximité des acteurs policiers nationaux et internationaux, leur conférant ainsi un rôle de courtier entre les pôles publics et pri-

vés de la gouvernance du cybercrime. Qu'il s'agisse de Microsoft, Symantec, Kaspersky ou Trend Micro, les ressources affectées par ces multinationales de la cybersécurité à des initiatives publiques de coopération s'avèrent largement supérieures aux moyens dont disposent la majorité des États.

La visualisation des données relationnelles permet de circonscrire rapidement certaines tendances évidentes, mais la densité des points et des liens représentés ne nous permet pas d'exploiter pleinement le potentiel de l'ARS. Au-delà de la description de certains agrégats de points et de leur localisation spatiale, l'examen d'un amas de liens entrelacés et superposés produit peu de sens tant qu'on ne l'analyse pas à l'aide d'outils de mesure visant à quantifier la cohésion de ce réseau et les diverses formes de centralité des acteurs qui le composent. Ces indicateurs mettent en lumière des résultats qui peuvent sembler de prime abord contre-intuitifs.

La mesure de la cohésion du réseau calcule la densité observée des liens existants par rapport aux liens possibles. Nous avons vu plus haut que notre matrice à deux dimensions permet d'accommoder un maximum de 33 507 liens potentiels. Elle n'en contient cependant que 2 102, soit 6,27 % de la densité maximale. Ce résultat vient ainsi infirmer la perception visuelle initiale d'un réseau hautement interconnecté. Qui plus est, la cohésion du réseau est fortement influencée par l'affiliation quasi-automatique de la majorité des acteurs gouvernementaux aux initiatives placées sous le patronage d'Interpol ou de l'UIT, même si la participation d'une majorité de pays membres s'avère bien plus formelle qu'effective. Nous sommes par conséquent en présence d'un réseau pouvant être défini par sa fragmentation et par un mode d'affiliation unique, qui représente la valeur médiane du nombre d'initiatives auquel les acteurs participent – la moyenne étant de 3,2 initiatives par acteur (avec une amplitude de 1 à 25). Dans une telle configuration, les acteurs capables de faire circuler l'information d'une initiative à l'autre et d'un groupe de membres à un autre, du fait de leurs appartenances multiples, disposent d'un pouvoir d'autant plus important qu'ils sont relativement peu nombreux à pouvoir connecter entre eux des archipels organisationnels caractérisés par leur isolement.

Trois mesures de centralité sont alors en mesure de nous indiquer quels acteurs et initiatives jouent un rôle prédominant dans la structuration de ce réseau : la centralité de degré, la centralité de proximité, et la centralité d'intermédiarité. Le tableau 3 présente les résultats de ces trois mesures pour les acteurs et les initiatives. La centralité de degré est la plus élémentaire, puisqu'elle assigne une valeur de centralité plus élevée aux acteurs ou aux initiatives qui disposent du plus grand nombre de connexions. Dans le cas d'un réseau d'affiliation comme le nôtre, la centralité de degré représente la somme des liens d'affiliation qu'un acteur entretient avec des initiatives ou le nombre

d'acteurs participants à une même initiative. Pour en rendre l'analyse plus lisible, nous exprimerons cette somme en un pourcentage afin de refléter le poids relatif du nombre de liens par rapport à la taille du réseau. Cette mesure purement cumulative de la connectivité fait ainsi apparaître le Royaume-Uni en tête des acteurs, avec des affiliations à 49 % des initiatives recensées, alors que la Chine et la Russie se classent respectivement 41ème et 148ème avec 22 % et 18 % des affiliations possibles. La première place du Royaume-Uni, qui devance de quelques points ses homologues européens, s'explique essentiellement par les liens de coopération privilégiés qu'elle entretien avec les pays du *Commonwealth* et ses quatre alliés anglo-saxons dans les activités de renseignement électronique (Australie, Canada, Nouvelle-Zélande, Royaume-Uni et USA formant le groupe des *Five Eyes*). En ce qui concerne les initiatives, c'est le FIRST qui réunit le plus grand nombre d'acteurs du réseau (39 %), suivi par quatre initiatives de l'UIT (l'*International multilateral partnership against cyber threats* ou IMPACT, et le projet *Child online protection* ou COP) et d'Interpol (le Complexe mondial Interpol pour l'innovation ou CMII, et le réseau d'échange d'informations i24/7). Les membres de FIRST sont en grande majorité des entreprises, qui ne peuvent à ce titre participer aux initiatives de l'UIT ou d'Interpol, réservées aux agences gouvernementales et à quelques multinationales.

Cependant, on observe entre ces deux dernières organisations une compétition implicite à travers la création de vitrines technologiques implantées en Asie (en Malaisie pour l'IMPACT et à Singapour pour le CMII d'Interpol) et destinées à les positionner comme des pôles incontournables de la coopération internationale anti-cybercriminalité. Bien que la centralité de degré soit généralement présentée comme une métrique appropriée permettant d'identifier les acteurs individuels qui accumulent beaucoup de capital social, elle reste insuffisante dans le cas des acteurs organisationnels ou des groupes d'acteurs tels que les initiatives de coopération étudiées ici [50]. En effet, le seul nombre d'initiatives auxquelles un acteur est affilié ne peut constituer un critère suffisant pour évaluer l'influence de ce dernier, particulièrement si ces initiatives s'avèrent marginales, de taille réduite ou réunissent des acteurs déjà côtoyés dans le contexte d'autres initiatives. De manière symétrique, des initiatives qui comptent un grand nombre d'organisations par ailleurs peu impliquées dans d'autres activités de coopération seront probablement moins influentes que des plateformes de coopération moins inclusives mais soutenues par des membres puissants et fort bien connectés.

On utilise donc la centralité de proximité pour mesurer la capacité d'un nœud du réseau à rejoindre avec le minimum d'efforts possibles l'ensemble des autres éléments qui composent ce dernier. Autrement dit, un acteur ou

50. Borgatti S., Jones C., Everett M., « Network measures of social capital », *Connections*, vol. 21, n° 2, 1998, pp. 27-36.

une initiative seront considérés comme occupant une position stratégique (pouvoir, accès à l'information, prestige, influence, etc.) dans le réseau s'ils sont globalement proches de toutes les autres composantes du réseau [51]. Les résultats obtenus avec ce deuxième indicateur sont considérablement modifiés, du moins pour les acteurs, puisque le premier rang est occupé par Microsoft, devant la Suisse, et que d'autres entreprises telles que Symantec ou Telefonica font également leur apparition dans le classement [52]. On voit également que le score normé de la Russie ou de la Chine est très proche de celui de Microsoft, par comparaison avec la différence séparant le premier et le dixième acteur pour la centralité de degré. Cela reflète la propriété de « petit monde » de la coopération internationale contre le cybercrime, où la fragmentation du réseau n'empêche pas ce dernier d'être composé de chaînes de liens relativement courtes entre chacun de ses membres. Contrairement aux acteurs, pour lesquels on voit des variations importantes apparaître selon les mesures de centralité utilisées, la centralité de proximité appliquée aux initiatives produit sensiblement le même classement que la centralité de degré. La place occupée par FIRST dans ce réseau est donc clairement attribuable à plusieurs dimensions, qui incluent le nombre d'acteurs affiliés mais aussi l'efficacité à mettre en relation des acteurs très diversifiés.

La troisième et dernière mesure appliquée dans le cadre de cette étude est la centralité d'intermédiarité. Celle-ci privilégie toujours une compréhension globale du positionnement, mais en se focalisant sur la capacité d'un acteur ou d'une initiative à servir d'intermédiaire unique entre des nœuds du réseau qui ne disposent d'aucune autre alternative pour communiquer [53]. Cela confère aux acteurs ou aux initiatives qui atteignent un score élevé d'intermédiarité la capacité d'exercer un plus grand contrôle sur leur environnement et d'être en retour moins dépendants de leurs pairs. On parle alors de courtiers ou d'intermédiaires, dont l'influence et le pouvoir seront moins déterminés par la quantité des liens tissés que par leur nature incontournable. On peut d'abord noter que les scores normés calculés pour les acteurs sont beaucoup plus faibles que pour les deux mesures précédentes, ce qui reflète encore une fois la propriété de « petit monde » et le pouvoir limité des acteurs se retrouvant en tête du classement : Microsoft n'est un intermédiaire inévitable qu'entre 6,2 % des chaînes de liens entre les membres de ce réseau, ce qui laisse de nombreuses options à la disposition des acteurs ou des initiatives qui ne souhaiteraient pas coopérer avec cette entreprise. Plus surprenante à première vue est la seconde place de l'association *Save the children*, mais celle-ci s'explique par sa capacité quasi-exclusive à raccorder l'initiative eNACSO au reste du réseau.

51. Chikhi N., *Calcul de centralité et identification de structures de communautés dans les graphes de documents*, Thèse de doctorat, Toulouse, Université Toulouse 3 Paul Sabatier, 2000, p. 21 ; Degenne A., Forsé M., *op. cit.*, p. 159.
52. Pour une discussion théorique et méthodologique approfondie de cette approche mise en œuvre dans le logiciel UCINET, voir Borgatti S. et Everett M., « Network analysis of 2-mode data », *Social Networks*, vol. 19, n° 3, 1997, pp. 243-269.
53. Degenne A., Forsé M., *op. cit.*, p. 159.

Tableau 3 : Acteurs et initiatives classés selon leurs scores de centralité

Centralité de degré				Centralité de proximité				Centralité d'intermédiarité			
Acteur	**Score**	**Initiative**	**Score**	**Acteur**	**Score**	**Initiative**	**Score**	**Acteur**	**Score**	**Initiative**	**Score**
1. Royaume-Uni	0.49	1. FIRST	0.39	1. Microsoft	0.82	1. FIRST	0.47	1. Microsoft	0.062	1. FIRST	0.484
2. Italie	0.43	2. IMPACT (UIT)	0.32	2. Suisse	0.80	2. COP (UIT)	0.46	2. Save the Children	0.057	2. APWG	0.203
3. Canada	0.41	3. COP (UIT)	0.32	3. Corée, Colombie, EAU	0.79	3. IMPACT (UIT)	0.43	3. Interpol	0.033	3. COP (UIT)	0.197
4. France	0.41	4. CMII (Interpol)	0.31	4. Brésil, Azerbaïdjan	0.78	4. i-24/7 (Interpol)	0.42	4. Canada	0.026	4. IMPACT (UIT)	0.122
5. USA	0.41	5. i-24/7 (Interpol)	0.30	5. Symantec, Telefonica	0.77	5. CMII (Interpol)	0.41	5. Suisse	0.022	5. CMII (Interpol)	0.083
6. Allemagne	0.39	6. APWG	0.17	6. Royaume-Uni, Canada, Interpol, USA	0.76	6. APWG	0.38	6 Symantec	0.021	6. i-24/7 (Interpol)	0.080
7. Hollande	0.39	7. Commonwealth Cybercrime Initiative	0.11	7. Australie, Italie, Hollande, Roumanie, France	0.75	7. Commonwealth Cybercrime Initiative	0.38	7. USA	0.020	7. Financial Coalition Against Child Pornography	0.060
8. Belgique	0.37	8. Global Alliance Against Child Sexual Abuse	0.08	8. Pologne, Allemagne, Belgique (+13 pays européens)	0.74	8. EC3	0.36	8. Corée	0.019	8. European NGO Alliance for Child Safety Online (eNACSO)	0.059
41. Chine	0.22	9. G8 24/7	0.08	9. Singapour, Malaisie, Inde, Japon	0.73	9. Global Project on Cybercrime	0.36	59. Chine	0.004	9. Commonwealth Cybercrime Initiative	0.048
148. Russie	0.18	10. EC3	0.07	10. Chine, Russie	0.72	10. Virtual Global Task Force	0.36	66. Russie	0.003	10. Global Prosecutors E-Crime Network	0.044

Note : les acteurs et initiatives figurant dans chaque colonne sont classés de manière décroissante et précédés de leur rang. Les scores de centralité sont directement calculés à partir du réseau 2-mode et sont présentés de manière normée afin de tenir compte des deux catégories distinctes d'acteurs présents dans ce type de réseaux. Il est important de préciser que ces trois mesures de centralité sont présentées dans un même tableau à des fins pratiques, et qu'il n'est pas possible de comparer les résultats obtenus par un même acteur sur chacune des trois dimensions, puisque les diviseurs ne sont pas les mêmes, ni même de comparer les scores obtenus par les acteurs et les initiatives pour la même mesure de centralité.

Du point de vue des initiatives, FIRST domine très nettement le classement de centralité d'intermédiarité, avec un score élevé de 48,4 % qui exprime la faible connectivité des acteurs qui y participent au reste du réseau. On est donc en présence d'une initiative qui contrôle l'accès à un nombre important d'acteurs (puisqu'elle obtient également le score le plus élevé de centralité de degré) qui ne disposent pour la majorité d'entre eux d'aucun autre canal de communication et d'échange avec les initiatives ou acteurs qui composent le réseau global. Cet écart entre FIRST et les initiatives d'Interpol et de l'UIT atteste du rôle privilégié que jouent dans cet assemblage coopératif les initiatives hybrides (public-privé), dont on connaît encore assez mal la contribution en matière de coopération internationale. Interpol, l'UIT ou encore Europol ont d'ailleurs pleinement pris la mesure de cette transformation, et ont conclu au cours des derniers mois des accords privilégiés avec de grandes entreprises informatiques afin de les intégrer de manière plus formelle dans leurs initiatives de lutte contre la cybercriminalité : Interpol a ainsi signé depuis 2012 des ententes avec NEC, Kaspersky, et Trend Micro afin d'équiper et partager des renseignements avec le CMII, alors qu'Europol s'est associé avec la Fédération bancaire de l'Union européenne, Microsoft, Kaspersky, Symantec, McAfee ou Sportradar afin de renforcer les capacités du *European cybercrime centre* (EC3).

Prolifération et coordination des initiatives de coopération dans un modèle coo-pétitif

L'évolution de la délinquance qui accompagne depuis un quart de siècle la révolution technologique suscitée par l'avènement d'internet produit à son tour une profonde reconfiguration des modalités du contrôle social. En prenant pour objet d'étude les mécanismes internationaux de la coopération policière et en adoptant une méthodologie encore peu mobilisée par la sociologie du *policing*, nous avons pu mettre en lumière quelques-unes des propriétés de la coopération internationale contre le cybercrime. Les modèles antérieurs en vigueur au XIX^e^ et au XX^e^ siècles (privatisation, bureaucratisation et hégémonie) semblent avoir cédé la place, pour cette forme de délinquance du moins, à un assemblage d'acteurs et de modalités relationnelles qui restent encore largement à étudier. Privatisation et bureaucratisation ont ainsi fusionné pour donner naissance à des configurations hybrides où agences gouvernementales, organisations internationales, entreprises et ONG tissent des liens collaboratifs afin d'échanger ressources et compétences. Le modèle hégémonique qui avait accompagné l'effort américain de guerre contre la drogue, puis contre le terrorisme, doit également être réévalué à l'aune des moyens considérables mobilisables par certains acteurs dominants du secteur privé. Microsoft, Symantec ou Telefonica disposent ainsi de capacités techniques et juridiques bien supérieures à celles de nombreux pays avec lesquels elles collaborent. Elles n'hésitent pas à les déployer de manière plus ou moins coordonnée avec

certaines institutions policières nationales et internationales afin de faire avancer leurs intérêts privés, qu'il s'agisse de maintenir la confiance des consommateurs dans leurs produits ou de les convaincre de la supériorité de leurs solutions sur celles de leurs compétiteurs. Même si elles valorisent fortement la collaboration avec les institutions publiques, quelques-unes de ces entreprises élaborent leurs propres stratégies de perturbation des réseaux criminels, comme c'est le cas par exemple de Microsoft et de son approche controversée de démantèlement des *botnets*, ces réseaux d'ordinateurs compromis qui constituent l'infrastructure du cybercrime [54]. Dans de rares cas, ces entreprises peuvent même choisir de faire prévaloir leurs intérêts sur ceux de leurs partenaires gouvernementaux, comme on l'a vu en 2014 dans la résistance opposée par Microsoft au FBI dans sa tentative d'obtenir des données personnelles stockées par l'entreprise dans un de ses serveurs basé en Irlande [55].

La nature résolument polycentrique des dispositifs contemporains de coopération internationale contre la cybercriminalité s'avère particulièrement adaptée à l'application de la méthodologie de l'ARS, qui permet d'en comprendre les propriétés structurelles. En l'absence d'un centre et d'une périphérie clairement délimités, le réseau global de coopération est composé d'archipels collaboratifs répondant à des logiques fonctionnelles ou géographiques très prégnantes : les ONG se consacrant à la lutte contre la pornographie juvénile et l'exploitation sexuelle restent finalement peu liées aux grandes entreprises essentiellement préoccupées par la croissance de la fraude en ligne, de la même façon que les acteurs européens, asiatiques, latino-américains ou appartenant au *Commonwealth* préfèrent s'associer à des initiatives locales où le nombre limité de participants favorise l'émergence d'un consensus. Loin d'assumer le statut de chef de file naturel que semblerait leur conférer une domination technologique historique sur l'Internet, les États-Unis semblent relativement désengagés des efforts multilatéraux de coopération, puisque des puissances moyennes telles que le Royaume-Uni, l'Italie, le Canada ou la France obtiennent des scores équivalents sur les trois dimensions de centralité. À la lumière des révélations faites par Edward Snowden depuis l'été 2013 sur les capacités de surveillance massives que la NSA met à la disposition des organismes fédéraux d'enquête tels que le FBI et la DEA, ce désintérêt pourrait s'expliquer par l'accès à des ressources internes suffisantes pour faire aboutir les enquêtes sans que le recours à des initiatives internationales de partage du renseignement soit jugé vital. On pourrait également formuler l'hypothèse qu'un mode de coopération bilatéral serait privilégié, ce qui expliquerait ces scores relativement faibles.

54. Lerner Z., « Microsoft the botnet hunter: The role of public-private partnerships in mitigating botnets », *Harvard Journal of Law & Technology*, vol. 28, n° 1, 2014, pp. 237-261.
55. Woollacott E., « Microsoft stands up to FBI over Customer data », Forbes.com, 23 mai 2014, accessible en ligne : http://www.forbes.com/sites/emmawoollacott/2014/05/23/microsoft-stands-up-to-fbi-over-customer-data/#1088fcda2fd6 (consulté le 8 juillet 2016).

Nous avons choisi d'inclure dans le tableau de présentation des résultats de centralité les scores obtenus par la Chine et la Russie. Ces deux puissances économiques émergentes qui sont fréquemment accusées de contribuer à l'insécurité de l'écosystème numérique par leurs activités d'espionnage ou l'indifférence de leurs autorités policières aux activités de piratage lancées de l'intérieur de leurs frontières se trouvent en effet reléguées à des rangs qui ne correspondent aucunement à leur poids technologique et économique réel. La faible connectivité de ces deux pays reflète la tension causée par le contexte de prédation et de compétition inhérent aux efforts soutenus de renseignement et d'espionnage politique et industriel dans le cyberespace, d'une part, et la nécessité de collaborer pour prévenir et combattre une cybercriminalité qui frappe indistinctement tous les acteurs de l'écosystème, d'autre part. On voit ici se dessiner concrètement les retombées néfastes d'une militarisation effrénée de l'Internet et d'un cyber-conflit généralisé sur la sécurité quotidienne des usagers « civils ». En ce qui concerne les acteurs privés, certains d'entre eux (notamment Microsoft et Symantec) investissent des ressources considérables dans les initiatives de coopération, alors que leurs compétiteurs qui disposent de moyens comparables (Apple et Google par exemple) paraissent impliqués de manière plus sporadique. Quant aux organisations internationales, certaines (notamment Interpol et l'UIT) semblent entretenir une rivalité implicite conduisant à une duplication importante des capacités de coordination. Ce constat peut être étendu à bien des initiatives régionales qui multiplient une offre de renforcement des capacités locales pléthorique en matière de lutte contre la cybercriminalité, dont la cohérence et l'efficacité restent encore difficiles à évaluer.

Bien qu'ils nous permettent de jeter un regard nouveau sur les modalités contemporaines de la coopération policière internationale contre la cybercriminalité, les résultats présentés dans cette contribution restent biaisés par le mode de collecte et la nature des données sur lesquelles ils s'appuient. Ils ne nous renseignent ainsi aucunement sur la réalité et l'intensité de l'implication des acteurs dans les diverses initiatives recensées, ni sur leurs intentions affichées ou cachées, dont l'interprétation est essentielle pour comprendre les stratégies participatives déployées. Les enjeux politiques et symboliques de l'affiliation à certaines initiatives ou de la collaboration avec des acteurs particuliers sont impossibles à déduire à partir de cette méthodologie, de la même manière que les négociations continuelles et les compromis inévitables qui en découlent ne peuvent être inférés à partir des données documentaires compilées. Enfin, il est indispensable de rappeler que les résultats présentés dans cet article se limitent aux initiatives multilatérales, et qu'un traitement méthodologique similaire des modalités bilatérales de coopération ou des enquêtes policières conjointes menées ces dernières années sous l'impulsion du FBI et d'Europol produirait certainement une image sensiblement différente. Mais plutôt que d'invalider les conclusions formulées précédemment, il nous sem-

ble que ces limites doivent être envisagées comme une invitation à mieux intégrer les approches qualitatives et quantitatives, qui ont parfois de la difficulté à s'extraire de traditions de recherche très cloisonnées. Là où les données ethnographiques riches permettent de saisir les rationalités guidant les décisions des acteurs sur le terrain, leurs cadres de référence culturels, leurs préférences, ou encore leurs expériences, les données documentaires traitées de manière systématique peuvent stimuler la formulation d'hypothèses sur les structures organisationnelles complexes qui découlent de cette multitude de décisions et d'interactions individuelles, suscitant par-là même des questions de recherche d'une grande fécondité à soumettre aux acteurs concernés.

Annexe : Liste des 51 initiatives de coopération policière analysées

24/7 Network (G8 - Sub-group on High-tech Crime, as of 2007)

2CENTRE - Cybercrimes Centres of Excellence for Training Research and Education

Action Innocence

Anti-Phishing Working Group

APEC Telecommunications and Information Working Group

ASEAN (Association of Southeast Asian Nations) - Ministerial Meeting on Transnational Crime

Asia Pacific Computer Emergency Response Team

Child Online Protection (ITU)

Ciberdelincuencia.org

Combating the Sexual Exploitation of Children on the Internet (COSEC)

Commonwealth Cybercrime Initiative

Commonwealth Working Group of Experts on Cybercrime

Cooperative Cyber Defence Centre of Excellence

COSPOL Internet Related Child Abuse Material Project (CIRCAMP)

Cybercrime Technology Information Network System (CTINS) Asia Pacific

CyberCrime@Octopus

CyberStorm

Eastern Partnership – Cooperation against Cybercrime

Eurojust Cybercrime Task Force

European Cybercrime Centre (EC3)

European Cybercrime Training and Education Group (ECTEG)

European Electronic Crime Task Force

European Financial Coalition against Commercial Sexual Exploitation of Children Online

European Multidisciplinary Platform Against Criminal Threats

European Network and Information Security Agency (ENISA)

European NGO Alliance for Child Safety Online (eNACSO)

European Union Cybercrime Task Force

Europol Platform for Experts

Family Online Safety Institute

Financial Coalition Against Child Pornography

FIRST - Forum for Internet Response and Security Teams

Global Action on Cybercrime (GLACY)

Global Alliance against Child Sexual Abuse

Global Project on Cybercrime (Phases 1-3)

Global Prosecutors E-Crime Network

I-24/7 (Interpol)

Information Security Commission of the Coordination Council

Inter-American Cooperation Portal on Cyber-Crime

International Association of Internet Hotlines (INHOPE)

International Centre for Missing and Exploited Children (ICMEC)

International Cybercrime Assistance Program

International Multilateral Partnership Against Cyber Threats (IMPACT)

INTERPOL Global Complex for Innovation (IGCI)

Joint Cybercrime Action Taskforce (J-CAT)

Kids' Internet Safety Alliance (KINSA)

Microsoft Digital Crimes Unit / Microsoft Cybercrime Center

Society for Policing of Cyberspace (POLCYB)

Stoneghost

Strategic Alliance Cyber Crime Working Group

Violent Crimes Against Children International Task Force

Virtual Global Task Force