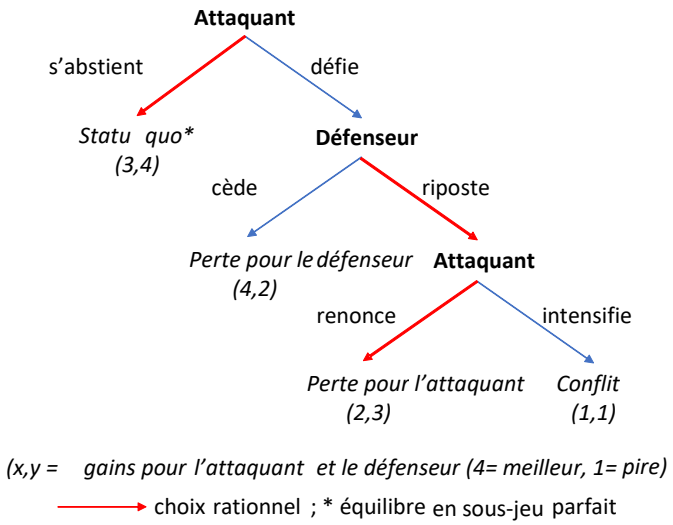
Cybersécurité : la coopération internationale requiert la réciprocité

Par Edouard Vidon, Céline Rochon

Les cyberattaques sont devenues une menace majeure, notamment pour la stabilité financière mondiale. En décryptant l'interaction stratégique entre les cybercriminels et leurs cibles, la théorie des jeux fournit des indications précieuses, mettant en évidence les limites et les effets secondaires de politiques de dissuasion non coordonnées et l'importance du partage des informations entre autorités publiques. La coopération internationale est essentielle et le G7 montre la voie.

Graphique 1 La théorie des jeux en application : Comment la dissuasion peut maintenir le statu quo



Note : Adapté de Zagare, 2019

Les pertes potentielles liées aux cyberattaques subies par les institutions financières ont été estimées entre 10 % et 50 % de leurs bénéfices dans un scénario extrême (Lagarde, 2018). L'importance de ces chiffres doit alerter les autorités responsables de la stabilité financière. Le cyber-risque fait cependant référence à un éventail de menaces dépassant largement le secteur financier. De fait, des cyberattaques réussies contre des infrastructures vitales telles que les hôpitaux, les aéroports et les télécommunications pourraient provoquer des perturbations généralisées avec des coûts humains et financiers importants. Heureusement, l'impact destructeur des attaques malveillantes a été limité jusqu'à présent, mais cela ne doit pas conduire à relâcher la vigilance.

Dans l'analyse du défi représenté par la cybersécurité, trois perspectives distinctes peuvent être adoptées :

- La perspective stratégique considère les cyberattaques dans le contexte d'une concurrence entre États, ou d'un conflit, la cyberguerre étant de plus en plus utilisée parallèlement à la guerre conventionnelle, ou même comme un substitut à celle-ci.

- La perspective opérationnelle se concentre sur la manière de garantir la sécurité et la continuité des différents systèmes des technologies de l'information et de la communication (TIC) par le biais de la détection des menaces, de la protection contre les attaques ainsi que du rétablissement et de la réponse après un incident. Cet aspect constitue une priorité pour les régulateurs et les superviseurs du secteur financier.

- Enfin, la perspective du bien public mondial examine les approches possibles pour renforcer la gouvernance internationale de la cybersécurité.

La théorie des jeux fournit des informations précieuses pour chacun de ces trois points de vue.

Au niveau stratégique, les experts en politique de défense ont souligné que les États, tout autant que les entreprises privées, imposent leur juridiction sur le cyberespace (Flournoy et Sulmeyer, 2018). Les cyberattaques commanditées par des États ont *de facto* été utilisées comme un instrument de guerre asymétrique. La théorie classique de la dissuasion met l'accent sur le coût d'un conflit et l'équilibre des forces comme éléments essentiels de la stabilité. En revanche, d'autres approches récentes (la théorie de la « dissuasion parfaite » : figure 1) soulignent l'importance de la valeur du *statu quo* et montrent que les rapports de forces asymétriques peuvent être très stables (Zagare, 2019). La principale conclusion de cette analyse est que dans les négociations avec un cyber-adversaire potentiel, il faut adopter la « coopération conditionnelle », c'est-à-dire menacer de répondre sur le même mode si un autre État ou acteur adopte un comportement non coopératif.

Les efforts de dissuasion peuvent détourner les attaques vers des cibles plus vulnérables

Des acteurs non étatiques ont également recours à la cybercriminalité. À cet égard, les outils de la théorie des jeux utilisés pour analyser les politiques de lutte contre le terrorisme (Sandler et Arce, 2007) sont intéressants. La littérature met en évidence les externalités associées à ces politiques. Les mesures de dissuasion prises pour protéger les autres cibles potentielles (gouvernements ou entreprises) peuvent présenter des externalités négatives si ces efforts de défense aboutissent à détourner les attaques vers des cibles plus vulnérables. En revanche, les mesures préventives (par exemple chercher à neutraliser les capacités criminelles ou geler des avoirs) ont des externalités positives qui bénéficient à toutes les cibles mais qui peuvent induire des comportements de passager clandestin. La mise en œuvre de telles mesures se heurte au risque d'une action collective insuffisante.

La figure 2 présente un jeu de coordination sur la cybersécurité : une action coopérative consiste à contribuer à l'identification et à la résolution des vulnérabilités en matière de sécurité. Une attitude non coopérative correspond à des mesures préventives insuffisantes et à un possible comportement de passager clandestin face aux efforts d'autres acteurs pour déployer une protection adéquate. Toutefois, le choix des mesures dépend également de l'étendue du partage des informations attendu de la part des autres acteurs et des coûts et avantages associés.
Deux versions de ce jeu peuvent être étudiées :

- La version du dilemme du prisonnier : les avantages à maintenir la confidentialité des informations relatives aux menaces provoquent une attitude non coopérative avec à la clé un résultat collectif inférieur.
- La version de la « chasse au cerf » : les bénéfices partagés provenant de la cyber-résilience sont supérieurs à ceux liés au maintien de la confidentialité des informations, mais l'équilibre coopératif continue d'exiger une confiance mutuelle.

Graphique 2. Jeu de coordination sur la cybersécurité

Dilemme du prisonnier :

Joueur A \ Joueur B	Coopérer	Ne pas coopérer
Coopérer	(2,2)	(0,3)
Ne pas coopérer	(3,0)	(1,1)*

Chasse au cerf :

Joueur A \ Joueur B	Coopérer	Ne pas coopérer
Coopérer	(3,3)*	(0,2)
Ne pas coopérer	(2,0)	(1,1)*

*(x,y) =Gains pour les joueurs A et B (3= meilleur, 0=pire) ; * équilibre de Nash*

Au niveau opérationnel de la mise en œuvre de la cybersécurité, la protection des TIC a également suscité l'intérêt des théoriciens. Un exemple classique est l'analyse de l'interaction dynamique attaquant/défenseur dans un jeu appliqué à l'origine à la sécurité physique : des agents avec des ressources limitées doivent décider, respectivement, où attaquer et où déployer des protections (par exemple des pare-feux, etc.). Une revue approfondie de la littérature (Do et al., 2017) montre dans quelle mesure la boite à outils de la théorie des jeux peut être utilisée pour relever des défis allant des attaques par déni de service à l'interaction entre la cybersécurité et la sécurité physique des infrastructures.

Il apparaît clairement que la gestion des cyber-risques et des ripostes possibles en matière de sécurité nécessite une compréhension approfondie des avantages comme des vulnérabilités. Par conséquent, la convergence vers une réglementation suffisamment exigeante de la gestion

des cyber-risques doit être favorisée afin d'éviter les arbitrages réglementaires et de garantir des normes adéquates.

Comment encourager le partage de l'information ?

Le problème du partage de l'information, qui implique un arbitrage entre avantages de l'échange de renseignements et protection des informations privilégiées mérite une attention particulière. La théorie des mécanismes d'incitation suggère l'utilisation de dispositifs d'enchères qui encouragent la révélation d'information. Le partage des informations s'avère particulièrement difficile s'agissant de la déclaration des cyber-incidents. À cet égard, la communication par les entités touchées, notamment entre gouvernements, reste entravée par une confiance limitée. Pour progresser dans ce domaine, il faudrait s'entendre sur une taxonomie commune des incidents et une convergence des obligations réglementaires de déclaration existantes pour obtenir un tableau plus complet et plus fiable de menaces en constante évolution.

Tableau 1 : Utiliser les outils de la théorie des jeux pour résoudre les problèmes de coordination

Séquence d'interactions	Problèmes	Outil associé de la théorie des jeux
Réputation des pays en matière de réciprocité en cas d'action collective	Crédibilité	Jeux répétés
Confiance dans le fait que tous les autres participants adhèrent à un accord de réciprocité	Asymétries d'information Aléa moral	Jeux à information incomplète
Étendue de la coopération	Formation de coalitions stables	Jeux de coalition
Bénéfices nets	Partage des gains et des coûts	Mécanismes de répartition

Les outils de la théorie des jeux (tableau 1) mettent en évidence les difficultés de la coopération internationale. L'incapacité des cibles (entreprises ou États) à coopérer incite les cyber-attaquants à rechercher les cibles les plus fragiles. En novembre dernier, lors du Forum de l'UNESCO sur la gouvernance de l'Internet, la France a lancé l'Appel de Paris pour la confiance et la sécurité dans le cyberespace. Cette déclaration de haut niveau condamne les cyber-activités malveillantes en temps de paix et appelle à un renforcement des normes internationales. En 2019, sous la présidence française du G7, la cybersécurité du secteur financier a été identifiée comme une priorité de la filière Finances. Une conférence de haut niveau sur le thème « Cybersécurité: coordonner la protection du secteur financier dans l'économie mondiale » a été organisée par la Banque de France en mai 2019. Les travaux actuels s'appuient sur les « Éléments fondamentaux » approuvés en 2016 par le G7, en mettant l'accent sur la gestion de crise. Dans le contexte du G7 et au-delà, une coalition des États désireux de garantir un cyberespace sûr et ouvert s'efforce de partager les bénéfices des politiques coopératives.