

# La monnaie électronique, arme de cyberguerre ?

Une guerre impliquant le clearing bancaire et les cartes de crédit ? Ce qui semble relever de l'utopie a déjà un début de réalité. *Ariel Wyler*

**Abrégé** Les économies ouvertes et technologiquement développées ont besoin d'un système de paiement efficace. Une panne nationale ou internationale du trafic des paiements peut rapidement se transformer en menace existentielle. Certains pays industrialisés, comme la Suisse, sont vulnérables aux pressions de nature financière. Si l'on veut se prémunir contre une crise éventuelle, il faut renforcer la capacité de résistance du trafic des paiements. La question est de savoir sous quelle forme.

Dans le conflit ukrainien, l'embargo sur les marchandises ne joue plus aujourd'hui qu'un rôle secondaire. Les sanctions financières, en revanche, sont importantes: elles ont provoqué une récession en Russie et l'offensive militaire a été freinée, du moins provisoirement.

La traçabilité de l'argent et la possibilité de surveiller les flux financiers permettent aujourd'hui d'appliquer des mesures d'embargo loin des territoires nationaux. Le conflit ne se déroule plus sur un théâtre d'opérations physique, mais dans le cyberspace, celui où s'opèrent les transactions financières.

Bien que la Suisse n'ait pas appliqué toutes les sanctions prises par l'UE et les États-Unis dans le conflit ukrainien, les entreprises qui y sont installées respectent l'embargo imposé aux affaires avec la Russie. Elles y sont poussées par la crainte, justifiée, de sanctions américaines ou européennes. La surveillance des flux financiers effectués par des intermédiaires sur Internet rend possible une mise en œuvre extraterritoriale des règles de l'UE et des États-Unis.

## L'arme des cartes de crédit

Allons plus loin et référons-nous aux méthodes connues du crime organisé sur Internet. Un exemple caractéristique est le chantage exercé au moyen d'un virus qui empêche un utilisateur d'accéder à sa propre installation sans le versement d'une certaine somme ou la réalisation d'une action précise. Imaginons alors un scénario qui peut paraître utopique à première vue.

A est une puissance économique dominante sur le plan des transactions aus-

si bien interbancaires (du fait de l'importance de sa monnaie) que des ménages. En effet, la majeure partie des opérations sur cartes de crédit y sont effectuées par des entreprises de l'État. Celui-ci, par ses organes de surveillance électronique, a aussi connaissance des paiements effectués par des sociétés de cartes de crédit et de toutes les transactions bancaires dans la monnaie nationale.

Admettons que l'État A décide d'utiliser les paiements électroniques comme moyen de pression sur l'État B. Il peut, par exemple, exclure ce dernier des compensations monétaires dans la devise nationale A. Il peut aussi décréter que les systèmes de cartes de crédit ne pourront pas être utilisés dans l'État B. Il peut encore placer dans les billetteries ou les systèmes de paiement par téléphone de B un virus qui bloque le compte de l'utilisateur final et ne le libère que si celui-ci reconnaît la législation de l'État A au lieu du droit en vigueur dans B. Ces trois actions peuvent, bien sûr, être simultanées.

Dans une cyberguerre, un État peut bloquer l'accès aux billetteries, comme en Russie.







On considérait, durant la Guerre froide, que là où Coca-Cola était implanté, les États-Unis l'étaient aussi. Camion de la firme en république Dominicaine.



Dans les économies à forte interconnexion internationale et trafic des paiements électroniques très développé, il y a fort à parier que certaines entreprises et autres acteurs seraient vite prêts à céder aux pressions, quand bien même leur gouvernement appellerait au contraire.

Si aucun de ces scénarios ne s'est vérifié jusqu'ici, certains éléments décrits ci-dessus, en revanche, sont déjà une réalité. La contamination par le ver informatique Stuxnet d'un programme nucléaire iranien théoriquement protégé ou le blocage de la chaîne française TV5 au nom d'un groupe islamiste montrent que même des systèmes réputés sûrs peuvent être infiltrés.

### Peut-on parler de guerre ?

Selon l'acception courante, la guerre stricto sensu est un conflit organisé et entretenu par un déploiement considérable d'armes et de violence. Une autre définition célèbre en est donnée par le théoricien militaire prussien Clausewitz: «La guerre n'est que le prolongement de la politique par d'autres moyens.» Cette formule n'inclut pas toutes les méthodes non diplomatiques visant à soumettre un adversaire à sa volonté.

Dans le passé, la définition traditionnelle et celle de Clausewitz étaient le plus souvent identiques. Parfois, ces guerres s'accompagnaient d'un embargo économique: c'est ce que Napoléon a fait avec le blocus continental ou les Britanniques en bloquant les mers lors de la Première Guerre mondiale. Une telle tactique vise à dicter sa volonté à l'adversaire en mettant son économie à genoux.

Avec le pacte Briand-Kellog de 1928 et l'adoption de la charte des Nations Unies au lendemain du deuxième conflit mondial, le droit de la guerre entre deux États a été fortement recadré. Il s'est limité aux actes de défense et aux actions collectives. Cela ne signifie pas que les États ou les sociétés vivent depuis lors en paix et dans la concorde. Elles cherchent plutôt à faire prévaloir leur volonté par d'autres moyens que militaires.

Voilà pourquoi, pendant la Guerre froide, les embargos sur les marchandises étaient la règle, sans s'accompagner pour autant d'actions militaires. Rappelons celui décrété par les États-Unis sur Cuba et celui que l'Occident avait institué sur les technologies de pointe à l'encontre des États membres du Pacte de Varsovie. Le succès de ces mesures fut toutefois limité: le Pacte de Varsovie n'a cessé d'exister

qu'après l'effondrement économique de l'Union soviétique, exténuée par la course aux armements des années quatre-vingts.

### Offensive avec Coca-Cola et Ford

Un autre moyen dont disposent les États est le pouvoir de projection («power projection»). Il s'agit de sa capacité à déployer, par des moyens rapides et efficaces, tout ou partie de sa puissance nationale – politique, économique, informationnelle ou militaire – sur des théâtres d'opération lointains, afin de réagir à des crises, de tenir des ennemis en respect ou d'assurer la stabilité d'une région.

Le plan Marshall en est un excellent exemple. Ce n'est pas seulement le soutien financier américain qui, après la Seconde Guerre mondiale, attachait les pays d'Europe de l'Ouest aux États-Unis, mais surtout les produits incarnant un certain style de vie. Sans trop exagérer, on peut affirmer que là où étaient Coca-Cola, Ford et General Electric, les États-Unis étaient aussi présents. Les droits de douane et les mesures techniques non tarifaires ont été la réplique à ce type d'invasion marchande. Les scénarios impliquant les systèmes de paiement, mentionnés plus haut, font également partie du pouvoir de projection.

### Domination par le maïs transgénique

Outre ces capacités de projection, d'importantes puissances commerciales ont beaucoup investi par le passé dans la diplomatie pour modifier les règles de jeu commerciales. Cela leur a permis de promouvoir leur propre économie ou de contourner la volonté d'autonomie d'autres États. Les débats autour du génie génétique en sont un exemple: c'est ainsi que des espèces de maïs étrangères brevetées évincent des variétés autonomes, cultivées sur le territoire national et librement disponibles.

Pour mener une telle bataille des marchandises, il faut que la production et le transport de biens soient clairement identifiables. Si l'origine n'apparaît pas et que le contrôle physique est impossible, les mesures commerciales restent inefficaces. Il n'est pas possible de promouvoir la puissance économique ni d'imposer un embargo en interdisant les livraisons.

De plus, tout embargo nécessite un lourd appareil de contrôle des marchandises. La loi suisse relative aux embargos

s'appuie sur un tel appareil. La coordination centrale de sa mise en œuvre incombe au Département fédéral de l'économie, de la formation et de la recherche (DEFR), anciennement Département de l'économie.

### L'argent perd son caractère anonyme

Curieusement, il existait jusqu'à récemment un bien qui n'était touché par aucun embargo: l'argent. Les Romains disaient déjà que l'argent n'a pas d'odeur. C'est un moyen idéal pour perdre dans l'anonymat des produits et des services identifiables. Pendant la Deuxième Guerre mondiale, l'Allemagne nazie avait pu (les États-Unis étaient au courant) changer des devises – dollars inclus – via la Banque des règlements internationaux et ainsi acquérir des biens d'États neutres. Après la guerre, seuls le négoce et l'échange d'or volé ont été remis en question, mais pas le clearing en tant que tel.

La lutte contre le terrorisme et le blanchiment d'argent, tout comme le trafic des paiements électroniques, font perdre à l'argent son anonymat. Sans aborder la question de la légalité, le cas de la banque Wegelin & Co. illustre la capacité de projection américaine basée sur la traçabilité de l'argent. Il a suffi de la confiscation d'avoirs électroniques auprès d'un établissement correspondant à Manhattan pour pousser Wegelin, et d'autres banques suisses dans son sillage, à se plier à la volonté du gouvernement américain.

L'introduction de la traçabilité parfaite des transactions monétaires et les restrictions dans le trafic d'espèces sonnent le glas du caractère anonyme de l'argent. Les autorités peuvent désormais non seulement clarifier ou interrompre une transaction isolée, mais également retracer le mouvement dans son intégralité, de la création monétaire à sa dernière utilisation. Pensée à l'origine comme un moyen de stabiliser le marché financier, la traçabilité procure également aux États un instrument pour filtrer et influencer des transactions de manière ciblée.

### La cyberguerre est meilleur marché

La seule existence d'un instrument de pouvoir ne signifie pas pour autant qu'il soit utilisé. Un agresseur potentiel vou-

dra, moyennant une capacité de projection, obtenir un avantage direct ou indirect qui promet, pour chaque unité mise en œuvre, un plus grand gain que le recours à d'autres facteurs, p. ex. d'ordre militaire.

De manière analogue au choix des objectifs et des moyens de traitement dans l'armée, il faut définir le stade final visé dans le cas d'une capacité de projection. Voici quelques objectifs possibles en lien avec le trafic des paiements :

- perturber ou détruire, puis s'approprier une place financière ou d'autres branches économiques essentielles à un État, ce qui menacerait son autonomie ;
- saper la confiance dans le gouvernement d'un pays pour obtenir un changement de régime ou faire pression sur lui afin qu'il accepte les conditions de l'agresseur ;
- s'emparer d'un substrat fiscal.

Là aussi, on peut imaginer une combinaison d'états finaux.

Les coûts directs de la guerre d'Irak sont estimés à un billion de dollars pour les États-Unis, qui n'en sont finalement pas sortis vainqueurs. Les dommages collatéraux ont été une société et une infrastructure anéanties. Toutes deux nécessiteront encore d'importants travaux de reconstruction. Appliquée à un État moderne, internationalement connec-

té, une fraction de ces moyens (mise en œuvre dans la capacité de projection financière) suffirait sans doute pour atteindre l'un des objectifs précités tout en conservant une infrastructure totalement intacte.

La capacité de projection au moyen de transactions financières est moins onéreuse pour l'agresseur potentiel et lui offre encore d'autres avantages. Contrairement aux « hommes verts » apparus lors de l'occupation de la Crimée, les exécutants qui veulent rester anonymes peuvent en outre se passer de cagoules. Même si un attaquant se fait connaître comme État, les différents acteurs, qu'ils exercent des sanctions financières ou programment une cyberattaque, restent anonymes. Ils se soustraient ainsi à d'éventuelles poursuites pénales ultérieures.

Si la guerre n'était donc que le prolongement de la politique par d'autres moyens, Clausewitz serait sans doute enchanté des possibilités offertes par la capacité de projection via le secteur financier.

### La Suisse doit renforcer sa résistance

Les armes existantes ne sont pas toutes utilisées et les menaces potentielles ne se concrétisent pas toujours. Actuellement, il est donc quasiment impossible

d'identifier un grave danger immédiat pour l'ensemble du trafic des paiements en Suisse. Il n'est cependant pas exclu que des dispositions visant à remettre en question l'autonomie et la souveraineté des décisions de la direction politique nationale soient prises ou brandies comme menace.

La Suisse doit s'efforcer de trouver les interdépendances critiques dans les processus qui accompagnent le trafic des paiements et de déterminer les moyens de renforcer son indépendance ainsi que sa résistance dans ce contexte. Cela peut notamment se faire à l'aide de systèmes de paiement nationaux redondants pouvant être détachés de l'étranger ou par la création d'un réseau garantissant une plus grande indépendance de la Suisse par rapport au clearing d'une monnaie de réserve dominante.



**Ariel Wyler**

Économiste, Secrétariat d'État aux questions financières internationales (SFI), Berne ; colonel, sous-chef d'état-major suppléant de l'instruction opérative