JEAN-LOUIS GERGORIN

Maître de conférences à Sciences Po Paris, gérant de la société de conseil en cybernétique et aérospatiale JLG Strategy

François Barrault, président de l'IDATE DigiWorld, fondateur et président de FDB Partners

J'aimerais maintenant accueillir Jean-Louis Gergorin, qui devait être avec nous aujourd'hui mais a eu quelques soucis. Il va parler de la confrontation dans l'espace numérique, du modèle alternatif à la guerre pour faire de la politique par d'autres moyens, en d'autres termes, comment les nouvelles guerres sont numériques plutôt que physiques.

Jean-Louis Gergorin

Bonjour, je suis très heureux et honoré de participer à cette conférence de la World Policy Conference d'Abou Dabi sur ce sujet clé qu'est l'avenir du numérique après la pandémie.

Clausewitz a dit que la guerre était la continuation de la politique par d'autres moyens. Par politique, il entendait toutes les actions humaines visant à assurer un contrôle ou une influence sur des populations et/ou sur des territoires. L'utilisation offensive de l'espace numérique est alors une forme moderne d'alternative à la guerre et de poursuivre la politique par d'autres moyens. Cette nouvelle méthode, cet outil d'influence et de contrôle politique, s'exerce par deux principaux modes d'utilisation de l'espace numérique, qui ont d'ailleurs une intersection non négligeable.

Le premier, c'est le *hacking*, l'intrusion informatique à des fins d'influence et de contrôle par sabotage, par intimidation, qui est en fait un sabotage virtuel par l'introduction de maliciels, de *malwares*, activables au moment que l'agresseur choisira et qui vise à intimider ou à préparer des actions futures. Il y a évidemment l'espionnage, qui est une activité tout à fait majeure qui a conduit à un énorme transfert de technologies vis-à-vis de certaines puissances qui ont, dans les vingt dernières années, rattrapé et même dépassé ceux qu'ils imitaient.

Enfin, Il y a la prédation, qui est une activité criminelle. Cela s'est notamment beaucoup développé depuis quelques années par le *ransomware*, c'est-à-dire le blocage du système informatique, accompagné ou non de la diffusion d'informations confidentielles saisies à cette occasion, pour obtenir une rançon importante qui est versée à des groupes cybercriminels. Ces groupes sont souvent très organisés et imbriqués dans des pays où ils opèrent en toute légalité, car ces pays n'ont pas signé la convention de Budapest contre le cybercrime. Ces groupes de *ransomware*, dont les noms sont connus – REvil, DarkSide, etc. –, n'agissent jamais contre les pays qui les abritent ou contre des pays alliés.

Voilà le paysage du *hacking*.

Le deuxième mode d'action, c'est la manipulation de l'information numérique sur Internet essentiellement, notamment des réseaux sociaux qui, comme chacun le sait, touchent des milliards d'humains et qui, par conséquent, ont un impact absolument dévastateur lorsqu'ils sont utilisés pour propager de fausses nouvelles.

Ces deux modes d'action peuvent se mélanger de façon assez aisée, comme cela a été démontré par le *hacking* qu'a subi l'Agence européenne des médicaments en décembre 2020, et qui a donné lieu à un vol d'informations sur toutes les correspondances internes des responsables de l'Agence européenne des médicaments évaluant le vaccin Pfizer.

Cela a ensuite donné lieu à une diffusion d'informations manipulées sur des forums de *hackers* et sur les réseaux sociaux, où certains des échanges étaient manipulés pour donner l'impression que les effets secondaires du Pfizer étaient beaucoup plus graves et beaucoup plus pernicieux que ce qui était apparu dans les évaluations authentiques, ceci à des fins, qui ne sont pas négligeables, de déstabiliser ce vaccin et donc de contribuer à des campagnes, qui se sont beaucoup développées sur Internet ensuite contre le vaccin, avec beaucoup de *fake news*, voire de théories complotistes. Ceci n'est pas sans conséquence puisqu'il y a littéralement des vies humaines qui sont en danger à partir du moment où il y a ces campagnes de *fake news* contre la vaccination.

Ce mode d'action se développe de plus en plus, et pas simplement par les grandes puissances qui ont des états-majors intégrés qui pratiquent à la fois le *hacking* et la manipulation de l'information numérique. Face à cela, il convient de réagir. Comment assurer la paix, la stabilité et la sécurité dans cet espace numérique qui est ainsi, en quelque sorte, déformé par cette utilisation offensive ? Je crois qu'il faut distinguer deux choses.

En ce qui concerne les réseaux sociaux, il n'y a pas d'action internationale possible, à mon sens. En revanche, il y a une régulation des réseaux sociaux qu'il appartient aux États de faire, notamment à ceux qui en ont la tutelle directe et je pense aux États-Unis, ou qu'il appartient aux réseaux sociaux eux-mêmes d'opérer par une autodiscipline pour lutter contre les *fake news*.

Deuxièmement, sur l'autre aspect, le *hacking,* qui peut donner lieu à des escalades pouvant devenir un jour hors de contrôle, c'est-à-dire des sortes de pandémie numérique, il est essentiel d'arrêter cette escalade. Mais pour arrêter cette escalade, je ne crois pas que les discussions purement limitées au numérique suffisent.

En un sens, le sommet Biden-Poutine du 16 juin, à Genève, a été très intéressant. Il a marqué un certain apaisement des tensions russo-américaines en général. Plus de 50 % des discussions ont été consacrées au problème du cyber à la suite d'une attaque de *ransomware* sur Colonial Pipeline aux États-Unis. Une certaine forme de modération s'est ensuivie de la part des groupes de *ransomware* abrités en Russie, qui n'ont plus effectué de grandes attaques dévastatrices du type de celle de Colonial Pipeline à partir de l'été, après une autre attaque qui a été bloquée sur Kaseya, au mois de juillet 2021.

Ce qu'il faut, c'est intégrer la discussion du sous-jacent géopolitique des conflits et les discussions sur la modération, la limitation de l'utilisation offensive du cyberespace. Il convient

d'avoir un forum pour cela, et je pense que le forum le plus légitime est celui du Conseil de sécurité des Nations Unies. Le président Macron avait lancé l'idée d'un sommet des membres du Conseil de sécurité qui n'a pas encore abouti. Elle pourrait être reprise en se focalisant sur ce sujet central de la sécurisation du cyberespace.

Pour cela, il faut évidemment que les chefs d'État ouvrent la voie à des conversations entre leurs experts numériques. Mais, parallèlement à ces discussions sur l'espace numérique, il faut qu'il y ait une discussion sur le sous-jacent géopolitique et stratégique, c'est-à-dire les conflits.

Il n'y aura de stabilité dans la relation cyber entre la Russie et les États-Unis et la Russie et les pays d'Europe occidentale, que si le sous-jacent géopolitique, qui est le *package* constitué par le conflit ukrainien et par les sanctions qui ont été décidées contre la Russie dans la foulée de ce conflit ukrainien, est abordé. Si ce sujet n'est pas abordé, nous n'arriverons pas à établir une forme de détente ou de stabilité dans le cyberespace entre la Russie et les pays occidentaux.

Le modèle, c'est ce que Nixon et Kissinger ont fait avec Brejnev et Gromyko en mai 1972, lors de la visite de Nixon à Moscou. Ils ont traité le sous-jacent géopolitique de leur opposition, globalement. Ensuite, évidemment, ils ont abouti à l'accord SALT 1, le premier accord de limitation des armements stratégiques. C'est le modèle que l'on doit poursuivre dans le cyberespace, nous n'y arriverons pas autrement. Mais c'est une voie qui, je pense, peut être prometteuse.

Traitons simultanément, de façon intégrée, le sous-jacent géopolitique des tensions entre un certain nombre de pays, notamment la Russie et la Chine d'une part, et les pays occidentaux d'autre part, et les manifestations dans l'espace numérique de ces conflits. Je crois que c'est une voie prometteuse. En tout cas, je plaide ardemment pour.