JEAN-LOUIS GERGORIN

Ancien directeur du Centre d'analyse, de prévision et de stratégie du ministère des Affaires étrangères

Thomas GOMART

I move now to Jean-Louis for his presentation. Jean-Louis, the floor is yours.

Jean-Louis GERGORIN

Merci Thomas. Je vais commencer en français pour simplement dire que la façon dont j'aborde le cyber est à la fois très liée à la cyber-sécurité, c'est-à-dire à l'ensemble des techniques et des analyses des attaques d'intrusions informatiques, qu'elles soient à des fins d'espionnage, ou de sabotage, ou d'extorsion financière, mais en même temps plus large et plus limitée.

En effet, pour moi, le cyber, – pour paraphraser Clausewitz –c'est une forme moderne,le plus souvent alternative à la guerre,de continuation de la politique par d'autres moyens.Je ne sous-estime évidemment pas le cyber en temps de guerre, utilisé pour paralyser informatiquement les systèmes adverses comme les Américains l'ont fait avec les défenses aériennes irakiennes en mars 2003,mais stratégiquement il s'intègre dans l'ensemble des moyens technologiques,dont la guerre electronique,visant à neutraliser les capacités de l'ennemi.

En revanche, le cyber en temps de paix correspond à une tendance majeure et en croissance constante, qu'on a vue hier, notamment lors du débat sur le *lawfare*, avec le très brillant exposé de la professeure Norodom, l'utilisation de moyens non létaux pour atteindre des objectifs politiques et stratégiques. Je vous rappelle que Sun-Tzu, le père historique de la stratégie, a dit : « Vaincre sans combattre est le comble du stratège. » Et donc c'est ce que nous allons discuter en passant à l'anglais.

Une fois le cyber défini, quels sont les principaux outils et supports, pour atteindre des objectifs stratégiques ? Il existe deux moyens principaux pour y parvenir. Ils sont en fait de plus en plus intégrés et de plus en plus perpétrés par les mêmes agresseurs. Le premier est le piratage, ou pénétration clandestine des réseaux informatiques pour y voler des informations, saboter ou extorquer de l'argent, par exemple avec des attaques dites de rançon.

Il existe cependant une autre voie importante qui consiste à atteindre un objectif politique, un objectif stratégique, par manipulation des médias numériques. Le plus courant de ces outils est la manipulation des principaux réseaux sociaux. On l'a vu, par exemple, lors de l'élection présidentielle américaine de 2016. Un certain nombre de faux comptes Facebook, Twitter ou Instagram, que les experts appellent des « sock puppets » ou chaussettes-marionnettes, ont été créés par de jeunes employés de l'Agence de Recherche sur Internet (IRA) de Saint-Pétersbourg, sous de fausses identités américaines. Ces « acteurs » de l'IRA défendaient souvent des positions politiques plutôt extrêmes. Ils se sont fait passer par exemple pour des militants du « black power » ou pour des tenants de la suprématie blanche, basés dans diverses régions des États-Unis. Interrogé sur l'IRA, Vladimir Poutine a rétorqué que cette organisation était totalement indépendante du gouvernement russe. Il a fait remarquer que la Fondation Soros, accusée depuis longtemps par les autorités russes de chercher à déstabiliser le régime, est un organisme indépendant du gouvernement américain...

L'importance de la manipulation des réseaux sociaux à des fins politiques est démontrée par le fait que Facebook et Twitter annoncent périodiquement la clôture de comptes pour « comportement inauthentique coordonné ».

Depuis 2016, nous sommes également confrontés à une nouvelle forme de manipulation de l'information numérique, les « deep fakes ». Il s'agit de faux fichiers audios et vidéos qui, grâce à un outil d'intelligence artificielle sophistiqué, Generative Adversarial Networks, sont très difficiles, voire impossibles à distinguer des fichiers authentiques. Ces fausses vidéos peuvent ensuite être largement diffusées via tous les supports numériques, services de messagerie,

réseaux sociaux, courriels, télévision, etc. Il existe une concurrence entre de nombreux centres de recherche, dont ceux des « méchants » évidemment, pour améliorer sans cesse la « qualité » de ces fausses vidéos. Pour vous donner un exemple concret, il serait très facile de créer un « deep fake » de Thierry de Montbrial ayant une discussion politiquement sensible, en tête-à-tête avec l'une des personnalités ici présentes à Marrakech. Il serait impossible de prouver que cette vidéo a été créée artificiellement. Pensez à l'utilisation potentielle de tels « deep fakes » dans les futures campagnes électorales.

Comment les grandes puissances ont-elles réagi face aux défis et aux opportunités du numérique ?

Depuis de nombreuses années, les Américains se sont principalement concentrés sur le renseignement, avec l'obsession de recueillir toutes les données possibles sur les personnes et les situations, bien plus d'ailleurs qu'ils ne pouvaient en traiter. Cette obsession de la NSA à tout savoir, partout, est allée jusqu'à des écoutes téléphoniques de la chancelière allemande discutant du menu d'un dîner avec son mari et au piratage du système informatique de l'Élysée. À mon avis, une grande partie de ces enregistrements a été manifestement excessive et pas vraiment amicale. Mais alors que les Américains se sont principalement axés sur le renseignement, d'autres puissances se sont concentrées sur la manipulation de l'information numérique. Et elles ont commencé plus tôt. Ceci explique la surprise des Américains en 2016 face à une opération numérique sophistiquée visant la campagne présidentielle, avec un usage combiné de piratage et de manipulation des réseaux sociaux.

Les Russes et les Chinois ont compris dès le début des années 2000, et même à la fin des années 1990, le potentiel du cyberespace, tant pour le piratage informatique que, plus tard, pour la manipulation des réseaux sociaux, pour obtenir des avantages stratégiques. Ils ont utilisé ce potentiel de différentes façons. Les Russes sont très intelligents, très brillants. Je ne pense pas qu'ils dépensent d'énormes ressources dans leurs opérations numériques. Il faut savoir que le budget de la défense russe est l'un des plus rentables au monde. Cette rentabilité est accrue dans le domaine du cyberespace par une excellente formation et de très bons experts.

Les Chinois se concentrent quant à eux sur deux priorités. La priorité interne vise une utilisation de plus en plus sophistiquée des outils numériques. Ils cherchent à protéger le régime en isolant le pays de l'Internet mondial. Ils mettent en place une surveillance numérique, quasi « orwellienne », de la population. La priorité externe a été un énorme effort de cyberintelligence économique qui a grandement aidé la Chine à combler son écart technologique avec les États-Unis.

L'essentiel de ma conclusion a trait à la montée rapide des menaces, due à trois facteurs combinés :

- la transformation numérique continue de tous les secteurs dans nos pays

- le constat évident que plus nous numérisons, plus nous sommes vulnérables

- le poids croissant, dans les menaces mondiales, des opérations parrainées par l'État et des activités cybercriminelles tolérées par l'État, telles que les logiciels de rançon.

Une entreprise privée ne peut pas y faire face à elle seule. Les États sont les seuls à disposer des capacités de renseignement nécessaires pour identifier les attaquants. Si vous ne savez pas qui vous attaque, il vous est beaucoup plus difficile de vous protéger. C'est pourquoi il est hautement souhaitable de mettre en place une bien meilleure interaction entre les entreprises et les gouvernements en matière de renseignement sur les menaces.

Il a souvent été demandé aux gouvernements de se doter d'un système de cyberdissuasion. Or le cyberespace ne permet pas de disposer d'une dissuasion semblable à la dissuasion nucléaire, sauf en cas de cyberattaque massive contre les infrastructures essentielles d'une nation. Mais face à une cyberguérilla quotidienne, vous devez démontrer votre capacité à blesser l'attaquant selon un mode de défense que j'appellerais réactif. Vous devez identifier votre adversaire et le punir, non pas pour provoquer une escalade, mais pour montrer que vous savez qui il est et pour le punir. C'est essentiel. Si nous n'avons pas cette possibilité, nous sommes paralysés.

En Europe, nous sommes confrontés à une récente menace très grave : le placement dans les infrastructures essentielles de pays clés (principalement dans le secteur de l'énergie) d'un nombre croissant d'implants contrôlés par

des États. Ces implants confèrent à ceux qui les contrôlent à distance la possibilité d'entraver matériellement les infrastructures concernées. L'objectif est l'intimidation et revient à indiquer silencieusement à nos dirigeants : « Vous savez que nous pouvons à tout moment interrompre pendant plusieurs heures l'alimentation électrique d'une de vos villes », comme cela s'est produit plusieurs fois dans un pays d'Europe de l'Est. C'est un défi majeur.

Pour faire face à tous ces défis, les Européens ont besoin à la fois d'une cyberdéfense plus forte et mieux coordonnée, d'une organisation internationale et d'un dialogue mondial pour contrer le nombre croissant de cyber-risques. C'est ce que le président Macron a commencé à communiquer avec son appel à la paix, à la sécurité et à la confiance dans le cyberespace. Il l'a communiqué il y a près d'un an, lors du Forum de la paix de Paris, mais aussi lors de discussions bilatérales avec les grandes puissances concernées.

Thomas GOMART

Thank you very much, Jean-Louis. I want to give Meir a chance to speak. Would you prefer to speak at the podium? There is a point of debate between Patrick and Jean-Louis about the role of companies so very briefly maybe on that topic, could you elaborate?

Patrick NICOLET

On the threat to intelligence, you are right. It is a very critical aspect. We have collaboration with a French state agency in Annecy that is providing us some information, CGHQ in the UK as well. It is not available everywhere. In India we have 110,000 people. I have zero information. However, this is complemented by the industry. We have our own large companies, such as Microsoft, Cisco, IBM, that process billions of events per day and are providing us with intelligence on the characteristics of different attacks.

We have an industry partnership that has been launched by Brad Smith, the general counsel of Microsoft called Tech Accord that brings together about 60 companies where we sit together and we exchange best practices and intelligence because ultimately it is a cost of doing business for us and there is no competitive advantage to gain. For the fun part, there is a hacker super league, so you can be informed and today I can tell you the group called Russian Bear is the number one in the super league because they can penetrate and migrate in a system in 30 minutes and the number two needs two and a half hours. It is crazy, but that is the way it works. Yes, we need the state, but the industry and the enterprise are developing their own means.

Thomas GOMART

I will let Jean-Louis respond to that after the presentation by Meir.