TOBBY SIMON

Fondateur et président de Synergia

Patrick Nicolet, directeur général de Linebreak SA, ancien directeur des technologies de Capgemini

Tout cela concerne l'exploitation des données et bien entendu, ces données doivent être protégées. Alors que faisons-nous en matière de cybersécurité ?

Tobby Simon, fondateur et président de Synergia

Merci Patrick et merci Thierry pour cette opportunité de prendre la parole à la World Policy Conference.

Nous vivons une époque très intéressante et l'architecture de sécurité actuelle a été aggravée par de multiples conflits, des contestations à propos de l'espace et l'adaptation rapide des technologies émergentes et avancées.

Dans le temps qui m'est imparti, je parlerai de trois choses distinctes.

La première sera les principes, la deuxième les menaces et la troisième la stratégie telle que nous la concevons.

J'évoquerai également brièvement la technologie quantique, moins l'informatique quantique qui est de la compétence d'un deuxième intervenant. Enfin, je partagerai quelques exemples d'IA et de Cyber, et ce que cela augure pour l'avenir.

Permettez-moi d'exposer les principes. Premièrement, nous pouvons tous convenir qu'il n'y a aucun air gap en matière de cybersécurité, qu'il s'agisse du périmètre, du cloud, de l'espace ou de l'edge. Deuxièmement, la surface de la cyber-vulnérabilité s'est étendue avec l'adoption des objets connectés et des capteurs. Cela est particulièrement vrai parce que nous vivons dans un monde où la plupart de nos infrastructures essentielles sont connectées. Troisièmement, le cryptage est partout et la sécurisation de notre cryptage est la clé de notre avenir numérique ou de notre réussite. Aujourd'hui, nous sommes davantage dans une économie de chiffrement, et un exemple à considérer serait celui des signatures numériques. Tout ce que nous validons numériquement est basé sur des signatures numériques et s'il existe une vulnérabilité à ce sujet, vous pouvez imaginer à quel point cela pourrait compromettre notre avenir.

Deuxièmement, je ferai brièvement allusion aux menaces. Les tendances mondiales en matière de cryptographie sont fortement compromises car des algorithmes puissants comme ceux de Shor et de Grover utilisent des ordinateurs tout aussi puissants, capables de déchiffrer n'importe quelle norme de cryptage. Ils le font avec des simulateurs quantiques, qui sont des ordinateurs très puissants capables de compromettre le cryptage. En ce qui concerne les ordinateurs quantiques, nous connaissions tous l'avènement de l'an 2000, on le connaissait à l'avance comme ayant lieu le 1er janvier 2000, mais personne ne sait avec certitude quand l'informatique quantique arrivera. En réalité, il s'agit de gérer l'inconnu.

Troisièmement, la majorité des données Web cryptées reposent sur une norme de cryptage appelée RSA 2048. Un ordinateur quantique doté de 4 099 qubits sera capable de briser les cryptages en quelques minutes.

Nous ne voyons pas une telle possibilité s'étendre au-delà de 2028-2030 mais cela pourrait s'être déjà produit. Les systèmes utilisant la cryptographie actuelle pour l'authentification à long terme sont menacés. Par exemple, considérez les données de santé et la possibilité qu'elles aient été compromises. De nombreux hôpitaux sont piratés parce que leurs données ont une très longue traîne. La cryptographie basée sur des algorithmes mathématiques est vulnérable aux attaques brutales. Lors d'un conflit entre nations, le réseau deviendra probablement la première cible de la ligne d'attaque. Il pourrait également y avoir d'autres raisons économiques impérieuses. Cela inclut les systèmes de défense nationale, les infrastructures essentielles, notamment les services publics comme l'électricité, les institutions financières, les soins de santé, l'armée – elles sont devenues des infrastructures cruciales lorsque nous parlons de sécurité nationale exhaustive.

La stratégie utilisée actuellement par les pirates informatiques est double : la première consiste à pirater sur le moment, à transformer en arme sur le moment. Si vous disposez de l'algorithme et de la cryptographie nécessaires pour décrypter, vous les utilisez comme arme sur le moment. La deuxième option consiste à pirater sur le moment, à stocker l'information et à l'utiliser comme arme plus tard lorsque vous aurez la possibilité de décrypter.

Fondamentalement, ce que nous essayons de proposer maintenant, c'est de passer d'un cryptage basé sur les mathématiques à la physique quantique, qui selon la science fondamentale est beaucoup plus difficile à déchiffrer. Ce postulat repose sur trois principes, dont l'un est le principe d'incertitude de Heisenberg, qui permet d'identifier les écoutes clandestines car l'onde s'effondre dès qu'il y a une intrusion. Deuxièmement, le théorème de non-clonage interdit la copie de données provenant d'états quantiques. Le troisième est le principe d'inégalité qui empêche l'incrustation d'attaques dans les systèmes physiques.

Je n'entrerai pas dans l'informatique quantique mais permettez-moi de parler de la technologie quantique, issue de la deuxième révolution quantique. Soit dit en passant, la première révolution quantique comprenait le nucléaire, les semi-conducteurs et les lasers. La seconde est davantage caractérisée par la manipulation de systèmes quantiques individuels, par exemple, l'écoute clandestine à l'aide de la distribution de clés quantiques, l'informatique quantique brisant le code RSA.

Je vais maintenant parler de l'IA et du cyber. Les systèmes d'IA constitueront l'un des vecteurs d'attaque contradictoire incontournables dans tous les domaines où l'IA accroît une action. Cela signifie qu'au moment où vous utilisez l'IA, une vulnérabilité se crée, c'est comme un boomerang qui peut éventuellement revenir vers vous. L'attaque implique une contamination et une manipulation des données, rendant ainsi l'IA très inefficace. Par exemple, permettez-moi de vous donner un scénario de conflit, disons que le domaine utilisé en IA est l'ISR, l'Intel en mode turbo. Le cas d'utilisation de l'IA serait pour la détection d'objets, qui seraient un actif, une personne et une référence, et l'attaque de l'IA serait l'extraction et l'évasion. Si vous regardez ce que les Russes ont pu faire avec leurs camps militaires dans le conflit actuel, vous y verrez en grande partie cette exploitation pour dissimuler la plupart des endroits où ils gardent leurs avions.

La combinaison de l'IA utilisée avec les HAPS (Pseudo-satellites à haute altitude), utiliser des satellites serait un peu plus difficile, mais les HAPS fonctionnant à une altitude beaucoup plus basse pourraient devenir des centres de données aériens. À l'avenir, lorsque nous passerons à un théâtre de guerre autonome, nous utiliserons davantage de systèmes HAPS, qui garantiront une communication rapide avec les personnes sur le terrain. Deuxièmement, avec

l'avènement de la technologie d'amélioration humaine, les êtres humains cybernétiques dotés d'implants dans leur corps sont capables de se connecter à un HAPS et de prendre des décisions beaucoup plus rapidement que s'ils appelaient un centre de commandement.

Enfin, en regardant vers l'avenir, il existe des systèmes neuronaux basés sur l'IA. Il existe l'IA et la quantique, mais le défi de l'IA ou le succès de la création d'un cryptage quantique dépend du niveau de complexité qu'on peut atteindre. Avec l'IA, on peut augmenter cette complexité en utilisant une technologie que nous appelons le texte chiffré. Actuellement, la norme la plus élevée est d'environ 2^{256}, mais avec des systèmes neuronaux basés sur l'IA, on peut augmenter la complexité du texte chiffré jusqu'à environ $2^{2,6 \text{ millions}}$. Voilà à quoi ressemblera l'avenir du cryptage de l'IA. Il y a des avantages et des inconvénients, mais c'est ainsi que je vois l'évolution de la technologie.

En conclusion, j'ai davantage insisté sur la partie militaire, car nous pensons que les organismes de défense sont probablement les plus rapides à adopter les technologies les plus avancées et que leur faire valider la technologie est une manière plus pragmatique d'aborder le marché en général.

Patrick Nicolet

Merci, Tobby. C'est un point intéressant qui rejoint ce que Kazuto disait sur la nécessité de politiques distinctes. J'en retiens deux points : en matière d'IA et de cybersécurité, vous avez décrit des systèmes complexes et plus ils sont complexes, plus la surface d'attaque augmente. D'après les présentations d'Ameena et de Tobby, on remarque que de nombreuses identités seront créées pour toutes ces machines. L'un des points majeurs de la cybersécurité est la gestion des identités et de l'accès aux systèmes sur cette base, c'est donc d'une grande complexité. Ensuite, on utilise également l'IA pour l'attaque, que l'on tente de neutraliser et malheureusement le parallélisme n'est pas encore en place. Nous avons donc des moments difficiles devant nous. Merci pour cet aperçu, Tobby.