Séance du 4 octobre 2022

ACADÉMIE DES TECHNOLOGIES
POUR UN PROGRÈS RAISONNÉ CHOISI PARTAGÉ

Conférence-débat d'Élisabeth Paté-Cornell
avec Bernard Barbier

GESTION DU RISQUE CYBERNÉTIQUE ET RÔLES DE L'INTELLIGENCE ARTIFICIELLE

La transformation numérique de toutes les organisations, entreprises, collectivités, gouvernements provoque un accroissement exponentiel du risque cybernétique. La gestion de ce risque, sa compréhension et sa maitrise sont devenues essentielles. Le travail présenté par Élisabeth Paté-Cornell est d'importance car il permet une évaluation rationnelle de ce problème complexe par une approche mathématique innovante utilisant un réseau bayésien. Il est ainsi devenu possible de traiter explicitement les incertitudes et d'apporter un peu de réalité et de rationalité dans la perception du cyber-risque. Une analyse quantitative réelle des cyber-risques permet de décider si ceux-ci sont acceptables et ainsi d'établir des priorités en fonction des contraintes financières. La probabilité de la menace peut être mesurée grâce à l'analyse des évènements collectés sur des dispositifs de type « pot de miel ». Le déploiement de réseaux intelligents au sein d'infrastructures vitales permet d'en augmenter fortement la fiabilité et l'efficacité. Toutefois, une connectivité accrue augmente fortement la vulnérabilité. La méthode de mesure des risques cyber proposée ici permet de réduire le conflit : connectivité/vulnérabilité. Les techniques d'apprentissage automatique (IA) apportent des outils qui vont changer assez fondamentalement les capacités de cyber-défense. Un robot de cyber-défense peut prendre des décisions automatiques de fermeture des portes dans le réseau et ainsi apporter une aide fondamentale à l'humain qui conserve la décision finale.

Élisabeth Paté-Cornell. Professeur à Stanford University, fondatrice et présidente du département de management des sciences et de l'ingénierie. Experte en analyse et gestion des risques d'ingénierie, spécialisée dans l'évaluation des renseignements et des risques d'attaques terroristes ainsi que dans le développement de modèles probabilistes d'analyse des risques avec des applications aux navettes de la NASA, aux plateformes pétrolières offshore et aux systèmes médicaux. Membre de la National Academy of Engineering américaine et de l'Académie des technologies.

Bernard Barbier. Ingénieur de formation, élève de l'École centrale de Paris, expert en cryptographie et en interception des communications. Ancien directeur du Commissariat à l'énergie atomique (CEA)/LETI, ancien directeur technique de la Direction générale de la sécurité extérieure (DGSE) puis ancien directeur de la cybersécurité et cyberdéfense du groupe Capgemini. Aujourd'hui président de la société BBCYBER et membre de l'Académie des technologies.

Analyse des risques cyber

Les principes de base de l'analyse du risque cyber pour une organisation reposent sur l'identification des scénarios de défaillance, le traitement explicite des incertitudes (statistiques et probabilités bayésiennes) et l'évaluation des ressources disponibles. La connaissance des différents types d'attaque est fondamentale : hameçonnage, dénis de service, hameçonnage téléphonique, malware, ransomware, attaque par force brute pour casser les mots de passe.

Les objectifs des modèles sont, pour une organisation spécifique, d'évaluer le cyber-risque, de décider si le risque est acceptable ou non, d'identifier les différentes options de gestion des risques, d'en évaluer les risques et les avantages et finalement d'établir des priorités en fonction des contraintes budgétaires.

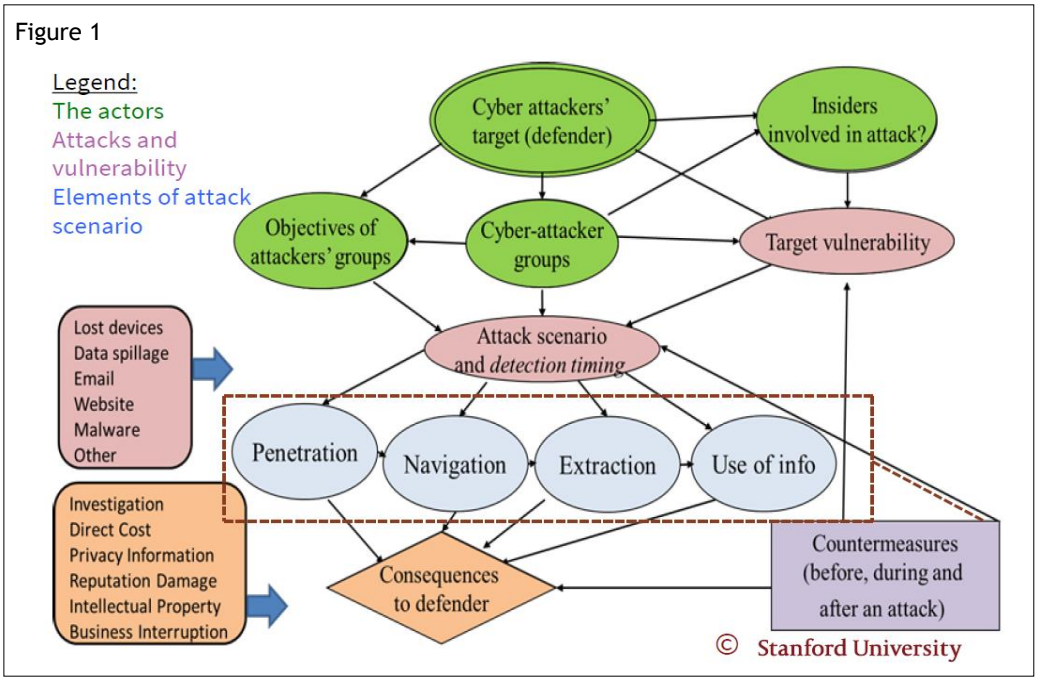
Quantification du risque cyber

La quantification repose sur une approche mathématique par la construction de courbes de risque (distribution de probabilité des pertes annuelles). Il existe trois façons de saisir les incertitudes dans les courbes de risque : une analyse statistique des données, une analyse probabiliste (basée sur des scénarios) et finalement les deux combinées.

Des informations spécifiques à la cible sont importantes pour le modèle de cyber-risque : la nature de l'organisation cible (hôpital vs entreprise spatiale), la nature des informations à protéger, la structure du système (physique et cybernétique), la connaissance des adversaires potentiels, les plus probables, les conséquences d'une attaque réussie et, pour les attaques connues, la constitution d'un ensemble des données statistiques pertinentes.

Pour les événements qui ne se sont peut-être pas encore produits, on utilise un réseau bayésien structuré pour modéliser des scénarios d'attaque potentiels (figure 1).

Figure 1



Réduction du risque cyber

La réduction du risque cyber est constituée :

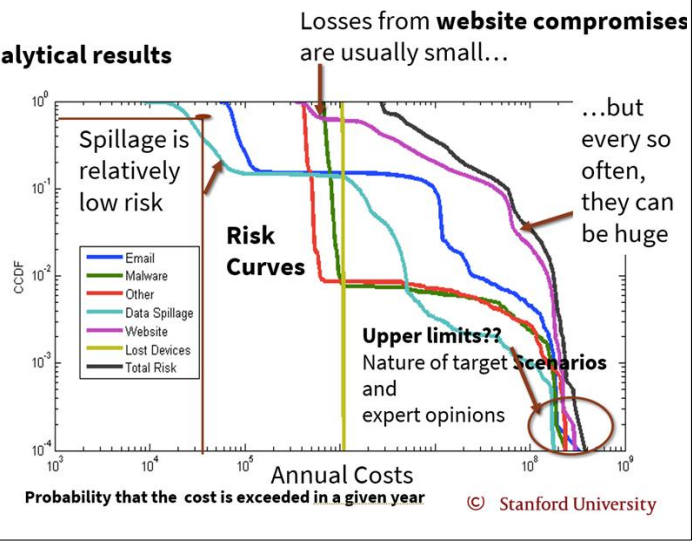
- Des mesures générales telles que le pare-feu, le chiffrement complet du disque, l'authentification à deux facteurs (ex. : mot de passe, code PIN, etc.), la détection de logiciels malveillants

- De la compartimentation du système telle que la protection (détection) contre la perte (exfiltration) de données, le filtrage des e-mails, l'utilisation de la biométrie.

L'efficacité de ces mesures dépend, entre autres, de la nature du système attaqué et du type d'attaque incluant par exemple le niveau de sophistication des attaquants.

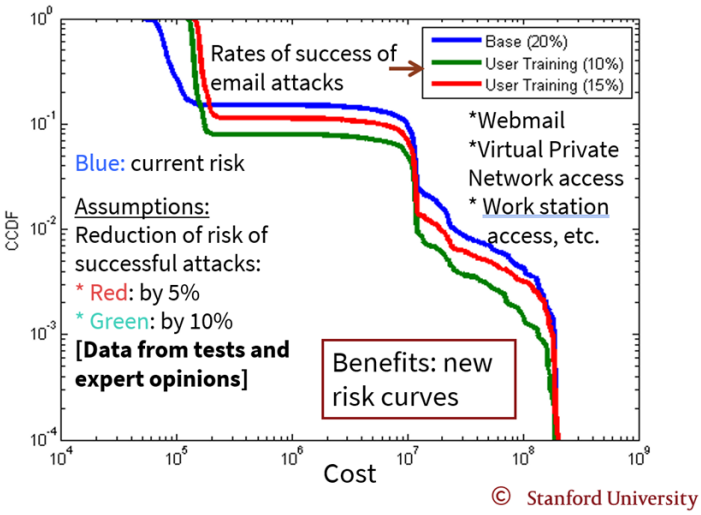
La quantification des risques et la comparaison des coûts des attaques sont essentielles (figure 2).

Figure 2



L'efficacité dès la formation des utilisateurs pour réduire le risque de type hameçonnage sont importants à évaluer (figure 3).

Figure 3



Un exemple important : les défis de la gestion des cyber-risques du réseau électrique « intelligent »

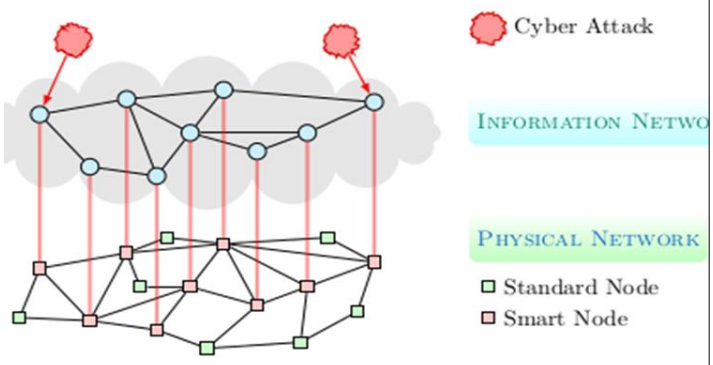
Les avantages du réseau électrique intelligent grâce à la communication par rapport à un réseau électrique traditionnel apportent une efficacité et une fiabilité supérieures en permettant aux systèmes du réseau et aux opérateurs de réagir intelligemment. Mais une connectivité accrue augmente la vulnérabilité et expose le réseau intelligent à de nouvelles menaces numériques telles que les attaques par déni de service, les vols de propriété intellectuelle ou/et de données personnelles et le sabotage d'une infrastructure critique de l'État.

- L'opérateur du système contrôle un réseau électrique physique : nœuds (générateurs, clients, sous-stations) et périphéries (lignes de transmission).

- L'opérateur peut choisir de connecter n'importe quel sous-ensemble de nœuds vers un réseau d'information du réseau intelligent superposé.

- Chaque nœud connecté permet une technologie Smart Grid mais devient également une vulnérabilité potentielle (figure 4).

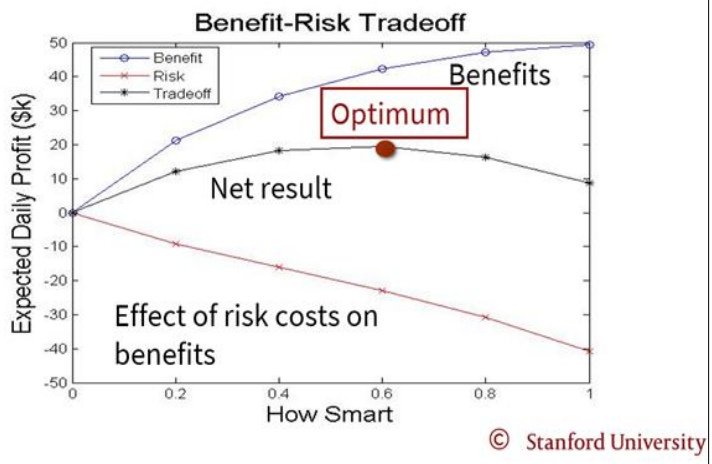
Figure 4



Smart Grid Cyber-Physical Network

Le modèle permet de trouver le point optimal lorsque le bénéfice marginal est égal au risque marginal (figure 5).

Figure 5



Une nouvelle approche prometteuse de la cyber-défense : les techniques d'apprentissage automatique (IA)

L'objectif est de générer des signaux précoces de menace d'attaque à l'aide de l'IA. Dans une équipe hybride qui dispose d'un « super expert », c'est-à-dire un robot associé à un humain, le robot prend la décision de laisser le circuit ouvert ou fermé sur la base d'un logiciel de contrôle de chaque porte et il fait appel à l'humain s'il y a trop d'incertitude. Une « porte » est une étape dans le processus d'attaque.

Il est essentiel d'identifier et de détecter les signaux à chaque étape de la « Cyber Kill Chain » (figure 6).

Le processus d'apprentissage et de mise à jour repose sur des données brutes obtenues à partir de « pots de miel ». Les fréquences d'attaque (comportements) sont utilisées pour identifier les menaces par l'analyse de fréquence des événements collectés dans les pots de miel. Par exemple, l'adresse IP qui apparaît le plus souvent est la plus susceptible d'être une menace.

Les hypothèses du modèle : les menaces et les demandes légitimes arrivent à la même porte suivant une répartition binomiale dans le temps. Le super agent (robot ou humain) doit décider si la barrière doit être ouverte ou fermée en fonction de l'utilité attendue des résultats et d'une préférence de risque (entrée dans le système pour le robot donc décision plus éclairée pour l'opérateur).

L'ouverture ou la fermeture de la porte est une décision de la part du super expert, par conséquent elle est contrôlable (figure 7).

Figure 6

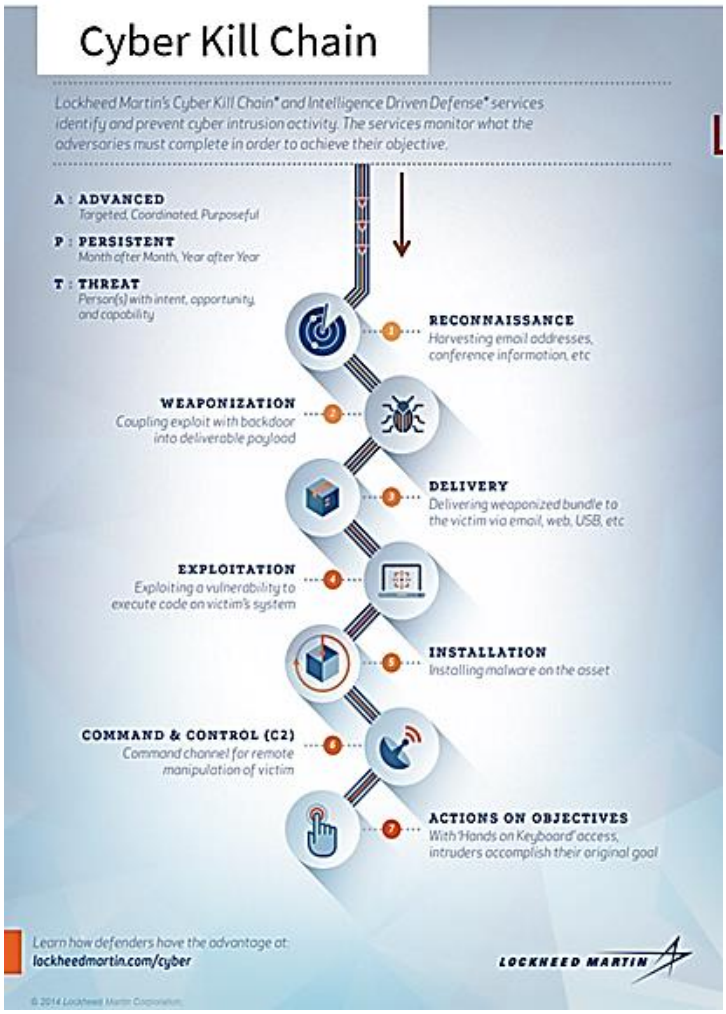
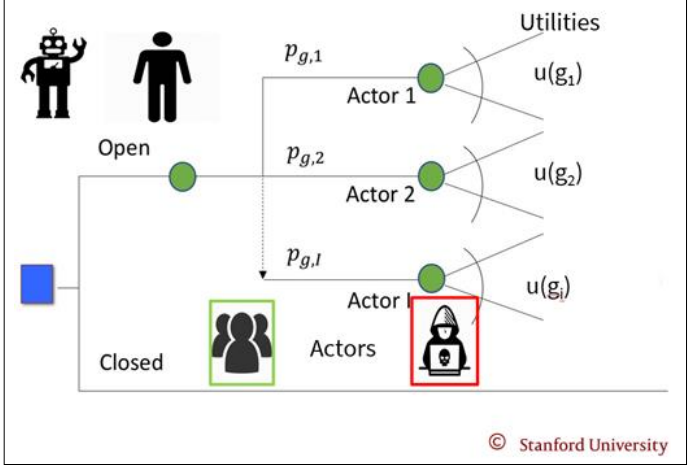


Figure 7



Le robot observe un signal entrant. Il obtient des informations de la base de données. Il décide d'ouvrir ou de fermer la porte de la manière optimale compte tenu de ce qu'il sait. Ensuite, le résultat est observé (légitime ou attaque) et la base de données est mise à jour. On peut utiliser les comportements comme signaux de menace pour prendre la décision d'ouvrir ou de fermer une porte (laisser l'acteur pénétrer ou non) au début de la chaîne de destruction, car le système apprend de ses opérations. Les décisions sont prises par le robot qui suit les informations et la règle de décision encodées dans la base de données ; ou par un humain qui prend des décisions lorsque le robot n'a pas assez d'informations pour prendre la meilleure décision et peut utiliser une attitude de risque différente.

Mots clés : apprentissage, bayésien, cybernétique, cyber-risque, cyber-vulnérabilité, robot

Citation : Élisabeth Paté-Cornell & Bernard Barbier. (2022). *Gestion du risque cybernétique et rôles de l'intelligence artificielle*. Les soirées de l'Académie des technologies. @

Retrouvez les autres parutions de l'Académie des technologies sur notre site

Académie des technologies. Le Ponant, 19 rue Leblanc, 75015 Paris. 01 53 85 44 44. academie-technologies.fr

Production du comité des travaux. Directeur de la publication : Denis Ranque. Rédacteur en chef de la série : Hélène Louvel. Auteurs : Bernard Barbier et Élisabeth Paté-Cornell. N°ISSN : en attente.